


**Post-Graduate Diploma in Cyber Security  
Fundamentals of Information Security  
(PGDCS-01)**

<b>Title</b>	Fundamentals of Information Security
<b>Advisors</b>	Mr. R.Thyagarajan, Head, Admn. & Finance and Acting Director, CEMCA Dr. Manas Ranjan Panigrahi, Program Officer(Education), CEMCA Prof. Durgesh Pant, Director- SCS&IT, UOU
<b>Editor</b>	Er. Saurav Joshi, Assistant Professor, Birla Insitute of Applied Sciences, Bhimtal
<b>Authors</b>	
<b>Block I&gt; Unit I, Unit II, Unit III &amp; Unit IV</b>	Ms. Priyanka Tewari, Technical Analyst, Infosys Technologies Ltd., Chandigarh
<b>Block II&gt; Unit I, Unit II, &amp; Unit III</b>	Ms. Priyanka Tewari, Technical Analyst, Infosys Technologies Ltd., Chandigarh
<b>Block II&gt; Unit IV</b>	Er. Ashutosh Bahuguna, Scientist, CERT-In
<b>Block III&gt; Unit I, Unit II, Unit III &amp; Unit IV</b>	Group Captain Ashok Katariya, Ministry of Defense, New Delhi
<b>ISBN:</b> 978-93-84813-88-8	
<b>Acknowledgement</b>	
The University acknowledges with thanks the expertixe and financial support provided by Commonwealth Educational Media Centre for Asia(CEMCA), New Delhi, for the preparation of this study material.	
 Uttarakhand Open University, 2016 © Uttarakhand Open University, 2016. Fundamentals of Information Security is made available under a Creative Commons Attribution Share-Alike 4.0 Licence (international): <a href="http://creativecommons.org/licenses/by-sa/4.0/">http://creativecommons.org/licenses/by-sa/4.0/</a> It is attributed to the sources marked in the References, Article Sources and Contributors section.	
Published by: Uttarakhand Open University, Haldwani	

<b>Expert Panel</b>	
<b>S. No.</b>	<b>Name</b>
<b>1</b>	<b>Dr. Jeetendra Pande, School of Computer Science &amp; IT, Uttarakhand Open University, Haldwani</b>
<b>2</b>	<b>Prof. Ashok Panjwani, Professor, MDI, Gurgaon</b>
<b>3</b>	<b>Group Captain Ashok Katariya, Ministry of Defense, New Delhi</b>
<b>4</b>	<b>Mr. Ashutosh Bahuguna, Scientist- CERT-In, Department Of Electronics &amp; Information Technology, Government Of India</b>
<b>5</b>	<b>Mr. Sani Abhilash, Scientist- CERT-In, Department Of Electronics &amp; Information Technology, Government Of India</b>
<b>6</b>	<b>Wing Commander C.S. Chawla, Ministry of Defense, new Delhi</b>
<b>7</b>	<b>Mr. Mukesh Kumar Verma, IT Consultant, Chandigarh</b>
<b>8</b>	<b>Mr. Pritam Dutt Gautam, IT Consultant, New Delhi</b>

# INDEX

1.1 LEARNING OBJECTIVES.....	1
1.2 HISTORY OF INTERNET.....	1
1.3 HOW INTERNET WORKS? .....	6
1.3.1 Hosts and Domain Names.....	7
1.3.2 Path Name and File Name .....	8
1.4 ADDRESSING SCHEME IN THE INTERNET .....	8
1.4.1 IP versions.....	8
1.4.2 IPv4 Addresses.....	9
1.4.2.1 Subnetting .....	9
1.4.2.2 Private Addresses.....	10
1.4.2.3 IPv4 address exhaustion.....	11
1.4.3 IPv6 Addresses.....	11
1.4.3.1 Private addresses .....	12
1.4.4 IP Subnetworks .....	12
1.4.5 IP address assignment .....	13
1.4.5.1 Methods.....	13
1.4.5.2 Uses of dynamic address assignment.....	13
1.4.5.3 Address autoconfiguration .....	14
1.4.5.4 Uses of static addressing.....	14
1.4.5.5 Conflict .....	14
1.4.6 Routing.....	14
1.4.6.1 Unicast addressing .....	15
1.4.6.2 Broadcast addressing .....	15
1.4.6.3 Multicast addressing .....	15
1.4.6.4 Anycast addressing .....	15
1.4.7 Public addresses .....	15
1.4.8 Modifications to IP addressing .....	15
1.4.8.1 IP blocking and firewalls .....	15
1.4.8.2 IP address translation .....	16

1.5 INTERNET SERVICE PROVIDER .....	16
1.5.1 Classification of ISP .....	16
1.5.1.1 Access providers ISP .....	17
1.5.1.2 Mailbox providers.....	17
1.5.1.3 Hosting ISPs.....	17
1.5.1.4 Transit ISP .....	17
1.5.1.5 Virtual ISPs.....	18
1.5.1.6 Free ISPs .....	18
1.5.1.7 Wireless ISP.....	18
1.6 DOMAIN NAME SYSTEM(DNS).....	18
1.6.1 How does it work? .....	18
1.6.1.1 Top-Level Domain(TLD) .....	19
1.6.1.2 Second-Level Domain .....	19
1.7 WORLD WIDE WEB(WWW).....	20
1.7.1 Is Internet and www similar? .....	21
1.7.1.1 The www.....	21
1.7.1.2 The Internet.....	21
1.8 APPLICATION OF INTERNET.....	22
1.9 SUMMARY .....	23
1.10 CHECK YOUR PROGRESS .....	24
1.11 ANSWERS TO CHECK YOUR PROGRESS .....	24
1.12 MODEL QUESTIONS .....	24
2.1 LEARNING OBJECTIVES.....	26
2.2 E-GOVERNANCE .....	26
2.2.1 Benefits of e-governance .....	26
2.2.2 Evolution of e-governance in India .....	28
2.3 AIM OF E-GOVERNANCE .....	30
2.4 STAGES OF E-GOVERNANCE.....	30
2.5 MODELS OF E-GOVERNANCE.....	30
2.5.1 Broadcasting Model.....	31
2.5.2 Comparative Analysis Model .....	32

2.5.3 Critical Flow Model.....	34
2.5.4 E-Advocacy Model .....	35
2.5.5 Interactive Service Model .....	37
2.6 LEGAL AND POLICY FRAMEWORK FOR FACILITATING ICT IN E-GOVERNANCE .....	38
2.7 SIGNIFICANCE OF E-GOVERNANCE .....	39
2.8 CHALLENGES IN THE IMPLEMENTATION OF E-GOVERNANCE .....	41
2.9 EVOLUTION IN E-GOVERNANCE AND MATURITY MODELS.....	43
2.9.1 Difference between E-Government and E-Governance .....	43
2.9.2 Levels of E-Governance .....	44
2.9.2 e-Governance maturity model.....	45
2.10 DIGITAL INDIA PROGRAM .....	48
2.10.1 Services .....	48
2.11 TOWARDS GOOD GOVERNANCE THROUGH E-GOVERNANCE MODELS .....	49
2.12 SUMMARY .....	49
2.13 CHECK YOUR PROGRESS .....	50
2.14 ANSWERS TO CHECK YOUR PROGRESS.....	50
2.15 MODEL QUESTIONS .....	50
3.1 LEARNING OBJECTIVES.....	52
3.2 STAGES IN E-GOVERNANCE.....	52
3.3 E-READINESS.....	53
3.3.1 Is the Technology Infrastructure Ready?.....	53
3.3.2 Is the Legal Infrastructure Ready?.....	53
3.3.3 Is the Institutional Infrastructure Ready?.....	53
3.3.4 Is the Human Infrastructure Ready? .....	53
3.3.5 Is the Technology framework Ready? .....	53
3.3.6 Is the Leadership and Strategic Thinking Ready? .....	54
3.4 BENEFITS OF E-GOVERNANCE .....	54
3.5 SUMMARY .....	56
3.6 MODEL QUESTIONS .....	57
4.1 LEARNING OBJECTIVES.....	58

4.2 INTRODUCTION .....	58
4.3 E-COMMERCE.....	58
4.3.1 Advantages of E-Commerce .....	59
4.3.2 Challenges in E-Commerce .....	59
4.4 E-COMMERCE BUSINESS MODELS .....	61
4.5 INFRASTRUCTURE .....	61
4.5.1 National Information Infrastructure.....	62
4.5.2 Message Distribution Infrastructure .....	62
4.5.3 Electronic Publishing Infrastructure .....	63
4.5.4 Business Services Infrastructure .....	63
4.5.5 Electronic Commerce Application.....	63
4.6 PAYMENT SYSTEMS .....	64
4.6.1 Electronic Funds Transfer.....	65
4.6.2 Digital Cash .....	65
4.6.3 e-cash .....	66
4.6.4 Credit card.....	66
4.6.5 Google Wallet .....	66
4.7 SUMMARY .....	67
4.8 CHECK YOUR PROGRESS .....	67
4.9 ANSWERS TO CHECK YOUR PROGRESS .....	68
4.10 MODEL QUESTIONS .....	68
BLOCK II .....	69
1.1 LEARNING OBJECTIVES.....	70
1.2 INTRODUCTION .....	70
1.2.1 Classification of Cyber Crimes .....	70
1.2.2 Reasons for Commission of Cyber Crimes.....	71
1.3 MALWARE AND ITS TYPES .....	72
1.3.1 Adware.....	72
1.3.2 Spyware.....	72
1.3.3 Browser hijacking software .....	73
1.3.4 Virus.....	74

1.3.5 Worms.....	74
1.3.6 Trojan Horse .....	75
1.3.7 Scareware.....	77
1.4 SUMMARY .....	78
1.5 CHECK YOUR PROGRESS .....	78
1.6 ANSWERS TO CHECK YOUR PROGRESS .....	79
1.7 MODEL QUESTIONS .....	79
2.1 LEARNING OBJECTIVES.....	80
2.2 KINDS OF CYBER CRIME .....	80
2.2.1 Cyber Stalking .....	80
2.2.2 Child Pornography.....	81
2.2.3 Forgery and Counterfeiting.....	81
2.2.4 Software Piracy and Crime related to IPRs .....	81
2.2.5 Cyber Terrorism.....	82
2.2.6 Phishing.....	82
2.2.7 Computer Vandalism .....	83
2.2.8 Computer Hacking.....	83
2.2.9 Creating and distributing viruses over internet.....	84
2.2.10 Spamming .....	84
2.2.11 Cross Site Scripting.....	85
2.2.12 Online Auction Fraud .....	86
2.2.13 Cyber Squatting .....	86
2.2.14 Logic Bombs.....	87
2.2.15 Internet Time Thefts .....	87
2.2.16 Web Jacking.....	88
2.2.17 Denial of Service Attack.....	88
2.2.18 Salami Attack.....	89
2.2.19 Data Diddling.....	89
2.2.20 Email Spoofing .....	90
2.3 SUMMARY .....	91
2.4 CHECK YOUR PROGRESS .....	91



2.5 ANSWERS TO CHECK YOUR PROGRESS .....	91
2.6 MODEL QUESTIONS .....	92
3.1 LEARNING OBJECTIVES.....	93
3.2 ORGANIZED CRIME.....	93
3.2.1 Types of organized crime groups.....	94
3.2.2 Classification of Cyber Crimes .....	95
3.2.3 Cyber Crime and Cyber Terrorism .....	95
3.2.4 Information Warfare and surveillance .....	95
3.3 IT ACT 2002.....	96
3.3.1 Objects and Reasons .....	96
3.3.2 Applicability of the Act .....	97
3.3.3 Exceptions to the Act.....	97
3.3.4 Basic Characteristics of the Act.....	97
3.3.5 Objectives of the Act .....	98
3.3.6 Definitions .....	98
3.3.7 Why was IT Act 2000 amended in 2008?.....	100
3.3.8 Data privacy .....	101
3.3.9 What are the responsibilities of a company handling personal data? .....	101
3.3.10 What is the punishment for cyber crimes?.....	102
3.3.11 Who can conduct RAIDS AND INVESTIGATION for Cybercrimes? .....	103
3.4 SUMMARY .....	103
3.5 CHECK YOUR PROGRESS .....	103
3.6 ANSWERS TO CHECK YOUR PROGRESS .....	104
3.7 MODEL QUESTIONS .....	104
4.1 LEARNING OBJECTIVES.....	105
4.2 INTRODUCTION .....	105
4.3 CYBER CRIME - CASE STUDIES.....	105
4.3.1 Cyber Stalking .....	105
4.3.1.1 Cyberstalking Facts.....	106
4.3.1.2 Examples of Cyberstalking.....	106
4.3.1.3 Guidelines for victim of Cyberstacking.....	106

4.3.1.4 Prevention Tips from Cyberstalking.....	107
Below are some tips useful for the prevention of cyber stalking: .....	107
4.3.1.5 Case Study on Cyber stalking.....	107
4.3.2 Ransomware.....	108
4.3.2.1 How does Cryptolocker work? .....	109
4.3.2.2 Prevention Tips from RANSOMWARE .....	109
4.3.2.3 Case studies on Ransomware.....	110
4.3.3 Silkroad .....	111
4.3.3.1 Case Studies on Silkroad .....	112
4.3.4 Phishing.....	113
4.3.4.1 Phishing Types.....	114
4.3.4.2 Anti-Phishing Groups .....	116
4.3.4.3 Legal Clause in Indian Penal Code.....	116
4.3.4.4 Case Studies in Phishing.....	117
4.3.5 419(Advance-Fee Fraud) Scam .....	117
4.3.5.1 What is 419 (Advance-fee Fraud) Scam? .....	117
4.3.5.2 Types of advance fee fraud and other Nigeria-related fraud emails.....	119
4.3.5.3 What should you do if you're a victim of 419 (Advance-fee Fraud) Scam.....	121
4.3.5.4 Protection Tips .....	122
4.3.5.5 Case Studies on 419 Scam .....	122
4.3.6 Unexpected prize and lottery.....	123
4.3.7 Dating and Romance Scam .....	125
4.4 LET US SUM UP .....	126
4.5 CHECK YOUR PROGRESS .....	127
4.6 ANSWERS TO CHECK YOUR PROGRESS .....	127
4.7 MODEL QUESTIONS .....	127
BLOCK III .....	128
1.1 LEARNING OBJECTIVES.....	129
1.2 INTRODUCTION .....	129
1.3 WHAT IS INFORMATION SECURITY?.....	129

1.3.1 Various Definitions .....	131
1.3.2 Information assurance .....	132
1.3.3 When Are We Secure?.....	132
1.4 MODELS FOR DISCUSSING SECURITY ISSUES .....	133
1.4.1 The Confidentiality, Integrity and Availability Triad.....	133
1.4.1.1 Confidentiality .....	133
1.4.1.2 Integrity.....	134
1.4.1.2 Availability .....	134
1.4.2 Relating the CIA triad to security .....	135
1.5 THE PARKERIAN HEXAD .....	135
1.5.1 Confidentiality, Integrity and Availability.....	136
1.5.2 Possession or Control.....	136
1.5.3 Authenticity .....	136
1.5.4 Utility.....	136
1.6 ATTACKS .....	136
1.6.1 Types of Attacks.....	136
1.6.1.1 Interception .....	137
1.6.1.2 Interruption .....	137
1.6.1.3 Modification.....	137
1.6.1.4 Fabrication .....	138
1.7 THREATS, VULNERABILITIES AND RISK .....	138
1.7.1 Threats.....	138
1.7.2 Vulnerabilities.....	138
1.7.3 Risk .....	138
1.7.4 Impact .....	139
1.8 CONTROLS .....	139
1.8.1 Physical .....	139
1.8.2 Logical .....	139
1.8.3 Administrative.....	140
1.9 DEFENSE IN DEPTH.....	140
1.9.1 Layers.....	141

1.10 INFORMATION SECURITY IN THE REAL WORLD .....	142
1.11 SUMMARY .....	142
1.12 CHECK YOUR PROGRES.....	143
1.13 ANSWERS TO CHECK YOUR PROGRES .....	144
1.14 MODEL QUESTIONS .....	144
2.1 LEARNING OBJECTIVES.....	145
2.2 INTRODUCTION .....	145
2.3 WHY IS INFORMATION SECURITY IMPORTANT?.....	145
2.4 INFORMATION, INFORMATION SECURITY AND INFORMATION SECURITY MANAGEMENT .....	147
2.4.1 What is information?.....	147
2.4.2 What is information security?.....	147
2.4.3 What is information security management? .....	149
2.5 INFORMATION SECURITY IMPERATIVES AND INCENTIVES .....	150
2.5.1 Imperatives.....	150
2.5.2 Incentives .....	151
2.6 INFORMATION ASSETS .....	151
2.6.1 Information in an e-business age .....	152
2.6.2 Scarcity and Shareability .....	152
2.6.3 Confidentiality, integrity and availability .....	154
2.7 PLANNING AN INFORMATION SECURITY MANAGEMENT SYSTEM.....	155
2.7.1 The Standard's approach to planning an ISMS .....	155
2.7.1.1 ISMS documentation .....	156
2.7.1.2 Asset identification .....	157
2.7.1.3 Risk assessment .....	157
2.7.1.4 Risk treatment .....	157
2.8 Other approaches to information security management .....	158
2.9 SETTING UP AN ISMS.....	159
2.10 ISMS DOCUMENTATION .....	159
2.10.1 Context, scope and information security policy .....	159
2.10.2 The Statement of Applicability .....	160

2.11 RISK ASSESSMENT AND ASSET IDENTIFICATION .....	160
2.11.1 A systematic approach to risk assessment .....	160
2.11.1.1 Threats, outcomes and impacts .....	160
2.11.1.2 Threats and vulnerabilities .....	162
2.11.1.3 Likelihood, impact and risk .....	163
2.11.1.4 Asset identification .....	164
2.12 THE PDCA CYCLE .....	165
2.13 SUMMARY .....	167
2.14 CHECK YOUR PROGRESS .....	167
2.15 ANSWERS TO CHECK YOUR PROGRESS .....	168
2.16 MODEL QUESTIONS .....	168
3.1 LEARNING OBJECTIVES.....	170
3.2 ELECTRONIC COMMERCE.....	170
3.3 HISTORY .....	170
3.4 BUSINESS MODEL .....	171
3.5 REVENUE MODEL.....	171
3.6 CONCERNS .....	171
3.6.1 Security .....	172
3.6.2 Privacy and confidentiality .....	172
3.6.3 Authenticity.....	172
3.6.4 Data integrity .....	172
3.6.5 Non-repudiation .....	173
3.6.6 Access control.....	173
3.6.7 Availability .....	173
3.7 SECURITY SOLUTIONS.....	173
3.7.1 Access and data integrity .....	173
3.7.2 Encryption.....	174
3.7.3 Digital certificates .....	174
3.7.4 Digital signatures .....	174
3.8 E-COMMERCE IDENTIFICATION AND IDENTIFICATION TYPES .....	174
3.9 IDENTIFICATION, AUTHENTICATION AND AUTHORIZATION.....	175

3.9.1 Identification .....	175
3.9.2 Authentication.....	175
3.9.3 Authorization .....	175
3.10 TYPES OF ECOMMERCE AUTHENTICATION.....	175
3.11 TYPES OOF BIOMETRIC AUTHENTICATION .....	176
3.12 OTHER FORMS OF AUTHENTICATION .....	177
3.13 SECURE ELECTRONIC TRANSACTION .....	178
3.13.1 History and development .....	178
3.13.2 Key features .....	179
3.13.3 Participants.....	179
3.13.4 How it Works.....	179
3.13.5 Dual signature .....	179
3.13.6 Digital signature.....	180
3.13.6.1 Explanation .....	180
3.13.6.2 How they work.....	181
3.13.7 Notions of security.....	182
3.13.8 Applications of digital signatures .....	182
3.13.8.1 Authentication.....	182
3.13.8.2 Integrity.....	183
3.13.8.3 Non-repudiation .....	183
3.14 ADDITIONAL SECURITY PRECAUTIONS.....	183
3.14.1 Putting the private key on a smart card.....	183
3.14.2 Using smart card readers with a separate keyboard.....	184
3.14.3 Other smart card designs.....	184
3.14.4 Using digital signatures only with trusted applications .....	184
3.14.5 Using a network attached hardware security module .....	184
3.15 DIGITAL SIGNATURES VERSUS INK ON PAPER SIGNATURES .....	185
3.15.1 Some digital signature algorithms .....	185
3.16 THE CURRENT STATE OF USE- LEGAL AND PRACTICAL.....	186
3.17 INDUSTRY STANDARDS .....	187
3.17.1 Using separate key pairs for signing and encryption .....	187

3.18 ANTIVIRUS SOFTWARE .....	187
3.18.1 Identification methods for viruses .....	188
3.18.2 Signature-based detection .....	188
3.18.3 Heuristics .....	189
3.18.4 Rootkit detection.....	189
3.18.5 Real-time protection.....	190
3.19 ISSUES OF CONCERN.....	190
3.19.1 Unexpected renewal costs.....	190
3.19.2 Rogue security applications .....	190
3.19.3 Problems caused by false positives.....	190
3.19.4 System and interoperability related issues.....	191
3.19.5 Effectiveness .....	192
3.19.6 New viruses.....	192
3.19.7 Alternative solutions .....	193
3.19.7.1 Hardware and network firewall .....	194
3.19.7.2 Cloud antivirus.....	194
3.19.7.3 Online scanning .....	195
3.19.7.4 Specialist tools .....	195
3.20 FIREWALL .....	195
3.21 COMPUTER FORENSICS .....	196
3.21.1 Use as evidence.....	197
3.21.2 Forensic process.....	198
3.21.2.1 Techniques .....	199
3.21.2.2 Cross-drive analysis .....	199
3.21.2.3 Live analysis .....	199
3.21.2.3 Deleted files .....	199
3.21.2.4 Volatile data.....	199
3.21.2.4 Analysis tools.....	200
3.21.2.5 Stochastic forensics.....	200
3.22 STEGANOGRAPHY .....	200
3.23 SUMMARY .....	201

3.24 CHECK YOUR PROGRESS .....	201
3.25 ANSWERS TO CHECK YOUR PROGRESS .....	202
3.26 MODEL QUESTIONS .....	202
4.1 LEARNING OBJECTIVES.....	204
4.2 INTRODUCTION .....	204
4.3 COMPUTER SECURITY AND ETHICS.....	205
4.3.1 The Moral Importance of Computer Security.....	205
4.3.2 How does computer security pose ethical issues? .....	205
4.3.3 Computer Security and National Security .....	206
4.4 ETHICAL ISSUES IN COMPUTER SECURITY.....	208
4.4.1 Hacking and Computer Crime .....	208
4.4.2 Cyberterrorism and Information Warfare .....	209
4.4.3 Moral Responsibilities of Information Security Professionals .....	210
4.5 INFORMATION PRIVACY AND ETHICS .....	210
4.5.1 What is Privacy and Why is It Important?.....	211
4.5.2 Information Technology and Privacy .....	211
4.6 PRIVACY ISSUES IN MODERN DATA MANAGEMENT .....	212
4.6.1 Internet Privacy .....	212
4.6.2 Record Merging and Matching and Data Mining .....	213
4.6.3 Privacy in Public .....	214
4.6.4 Biometric Identification.....	214
4.6.5 Ubiquitous Computing and Ambient Intelligence .....	215
4.7 TACTICS TO ENSURE COMPUTER SECURITY AND MAINTAIN PRIVACY .....	215
4.8 SUMMARY .....	216
4.9 CHECK YOUR PROGRESS .....	216
4.10 ANSWERS TO CHECK YOUR PROGRESS .....	217
4.11 MODEL QUESTIONS .....	217
References, Article Sources and Contributors .....	218



## **BLOCK I**

## UNIT I: INTERNET

### ***1.1 LEARNING OBJECTIVES***

After going through this unit, you will be able to:

- Know the evolution of Internet.
- Understand the working of the Internet.
- Understand Domain Name System.
- Understand the addressing scheme in the Internet.
- Know the different versions of IP.
- Know the working of an ISP.
- Differentiate www with the Internet.

### ***1.2 HISTORY OF INTERNET***

The Internet was the result of some visionary thinking by people in the early 1960s who saw great potential value in allowing computers to share information on research and development in scientific and military fields. J.C.R. Licklider of MIT first proposed a global network of computers in 1962, and moved over to the Defense Advanced Research Projects Agency (DARPA) in late 1962 to head the work to develop it<sup>1</sup>. Leonard Kleinrock of MIT and later UCLA developed the theory of packet switching, which was to form the basis of Internet connections. Lawrence Roberts of MIT connected a Massachusetts computer with a California computer in 1965 over dial-up telephone lines. It showed the feasibility of wide area networking, but also showed that the telephone line's circuit switching was inadequate. Kleinrock's packet switching theory was confirmed. Roberts moved over to DARPA in 1966 and developed his plan for ARPANET. These visionaries and many more left unnamed here are the real founders of the Internet.

The Internet, then known as ARPANET, was brought online in 1969 under a contract let by the renamed Advanced Research Projects Agency (ARPA) which initially connected four major computers at universities in the southwestern US (UCLA, Stanford Research Institute, UCSB, and the University of Utah). The contract was carried out by BBN of Cambridge, MA under Bob Kahn and went online in December 1969. By June 1970, MIT, Harvard, BBN, and Systems Development Corp (SDC) in Santa Monica, Cal. were added. By January 1971, Stanford, MIT's Lincoln Labs, Carnegie-Mellon, and Case-Western Reserve U were added. In months to come, NASA/Ames, Mitre, Burroughs, RAND, and the U of Illinois plugged in. After that, there were far too many to keep listing here.

The Internet was designed to provide a communications network that would work even if some of the major sites were down. If the most direct route was not available, routers would direct traffic around the network via alternate routes.

---

<sup>1</sup> <http://www.walthowe.com/navnet/history.html>

The early Internet was used by computer experts, engineers, scientists, and librarians. There was nothing friendly about it. There were no home or office personal computers in those days, and anyone who used it, whether a computer professional or an engineer or scientist or librarian, had to learn to use a very complex system.

E-mail was adapted for ARPANET by Ray Tomlinson of BBN in 1972. He picked the @ symbol from the available symbols on his teletype to link the username and address. The telnet protocol, enabling logging on to a remote computer, was published as a Request for Comments (RFC) in 1972. RFC's are a means of sharing developmental work throughout community. The ftp protocol, enabling file transfers between Internet sites, was published as an RFC in 1973, and from then on RFC's were available electronically to anyone who had use of the ftp protocol.

Libraries began automating and networking their catalogs in the late 1960s independent from ARPA. The visionary Frederick G. Kilgour of the Ohio College Library Center (now OCLC, Inc.) led networking of Ohio libraries during the '60s and '70s. In the mid 1970s more regional consortia from New England, the Southwest states, and the Middle Atlantic states, etc., joined with Ohio to form a national, later international, network. Automated catalogs, not very user-friendly at first, became available to the world, first through telnet or the awkward IBM variant TN3270 and only many years later, through the web. See The History of OCLC

The Internet matured in the 70's as a result of the TCP/IP architecture first proposed by Bob Kahn at BBN and further developed by Kahn and Vint Cerf at Stanford and others throughout the 70's. It was adopted by the Defense Department in 1980 replacing the earlier Network Control Protocol (NCP) and universally adopted by 1983.

The Unix to Unix Copy Protocol (UUCP) was invented in 1978 at Bell Labs. Usenet was started in 1979 based on UUCP. Newsgroups, which are discussion groups focusing on a topic, followed, providing a means of exchanging information throughout the world . While Usenet is not considered as part of the Internet, since it does not share the use of TCP/IP, it linked unix systems around the world, and many Internet sites took advantage of the availability of newsgroups. It was a significant part of the community building that took place on the networks. Similarly, BITNET (Because It's Time Network) connected IBM mainframes around the educational community and the world to provide mail services beginning in 1981. Listserv software was developed for this network and later others. Gateways were developed to connect BITNET with the Internet and allowed exchange of e-mail, particularly for e-mail discussion lists. These listservs and other forms of e-mail discussion lists formed another major element in the community building that was taking place.

In 1986, the National Science Foundation funded NSFNet as a cross country 56 Kbps backbone for the Internet. They maintained their sponsorship for nearly a decade, setting rules for its non-commercial government and research uses.

As the commands for e-mail, FTP, and telnet were standardized, it became a lot easier for non-technical people to learn to use the nets. It was not easy by today's standards by any means, but it did open up use of the Internet to many more people in universities in particular. Other departments besides the libraries, computer, physics, and engineering departments found ways to make good use of the nets--to communicate with colleagues around the world and to share files and resources.

While the number of sites on the Internet was small, it was fairly easy to keep track of the resources of interest that were available. But as more and more universities and organizations--and their libraries-- connected, the Internet became harder and harder to track. There was more and more need for tools to index the resources that were available.

The first effort, other than library catalogs, to index the Internet was created in 1989, as Peter Deutsch and Alan Emtage, students at McGill University in Montreal, created an archiver for ftp sites, which they named Archie. This software would periodically reach out to all known openly available ftp sites, list their files, and build a searchable index of the software. The commands to search Archie were unix commands, and it took some knowledge of unix to use it to its full capability.

At about the same time, Brewster Kahle, then at Thinking Machines, Corp. developed his Wide Area Information Server (WAIS), which would index the full text of files in a database and allow searches of the files. There were several versions with varying degrees of complexity and capability developed, but the simplest of these were made available to everyone on the nets. At its peak, Thinking Machines maintained pointers to over 600 databases around the world which had been indexed by WAIS. They included such things as the full set of Usenet Frequently Asked Questions files, the full documentation of working papers such as RFC's by those developing the Internet's standards, and much more. Like Archie, its interface was far from intuitive, and it took some effort to learn to use it well.

Peter Scott of the University of Saskatchewan, recognizing the need to bring together information about all the telnet-accessible library catalogs on the web, as well as other telnet resources, brought out his Hytelnet catalog in 1990. It gave a single place to get information about library catalogs and other telnet resources and how to use them. He maintained it for years, and added HyWebCat in 1997 to provide information on web-based catalogs.

In 1991, the first really friendly interface to the Internet was developed at the University of Minnesota. The University wanted to develop a simple menu system to access files and information on campus through their local network. A debate followed between mainframe adherents and those who believed in smaller systems with client-server architecture. The mainframe adherents "won" the debate initially, but since the client-server advocates said they could put up a prototype very quickly, they were given the go-ahead to do a demonstration

system. The demonstration system was called a gopher after the U of Minnesota mascot--the golden gopher. The gopher proved to be very prolific, and within a few years there were over 10,000 gophers around the world. It takes no knowledge of unix or computer architecture to use. In a gopher system, you type or click on a number to select the menu selection you want.

Gopher's usability was enhanced much more when the University of Nevada at Reno developed the VERONICA searchable index of gopher menus. It was purported to be an acronym for Very Easy Rodent-Oriented Netwide Index to Computerized Archives. A spider crawled gopher menus around the world, collecting links and retrieving them for the index. It was so popular that it was very hard to connect to, even though a number of other VERONICA sites were developed to ease the load. Similar indexing software was developed for single sites, called JUGHEAD (Jonzy's Universal Gopher Hierarchy Excavation And Display).

In 1989 another significant event took place in making the nets easier to use. Tim Berners-Lee and others at the European Laboratory for Particle Physics, more popularly known as CERN, proposed a new protocol for information distribution. This protocol, which became the World Wide Web in 1991, was based on hypertext--a system of embedding links in text to link to other text, which you have been using every time you selected a text link while reading these pages. Although started before gopher, it was slower to develop.

Marc AndreessenThe development in 1993 of the graphical browser Mosaic by Marc Andreessen and his team at the National Center For Supercomputing Applications (NCSA) gave the protocol its big boost. Later, Andreessen moved to become the brains behind Netscape Corp., which produced the most successful graphical type of browser and server until Microsoft declared war and developed its MicroSoft Internet Explorer.

Since the Internet was initially funded by the government, it was originally limited to research, education, and government uses. Commercial uses were prohibited unless they directly served the goals of research and education. This policy continued until the early 90's, when independent commercial networks began to grow. It then became possible to route traffic across the country from one commercial site to another without passing through the government funded NSFNet Internet backbone.

Delphi was the first national commercial online service to offer Internet access to its subscribers. It opened up an email connection in July 1992 and full Internet service in November 1992. All pretenses of limitations on commercial use disappeared in May 1995 when the National Science Foundation ended its sponsorship of the Internet backbone, and all traffic relied on commercial networks. AOL, Prodigy, and CompuServe came online. Since commercial usage was so widespread by this time and educational institutions had been paying their own way for some time, the loss of NSF funding had no appreciable effect on costs.

Today, NSF funding has moved beyond supporting the backbone and higher educational institutions to building the K-12 and local public library accesses on the one hand, and the research on the massive high volume connections on the other.

During this period of enormous growth, businesses entering the Internet arena scrambled to find economic models that work. Free services supported by advertising shifted some of the direct costs away from the consumer--temporarily. Services such as Delphi offered free web pages, chat rooms, and message boards for community building. Online sales have grown rapidly for such products as books and music CDs and computers, but the profit margins are slim when price comparisons are so easy, and public trust in online security is still shaky. Business models that have worked well are portal sites, that try to provide everything for everybody, and live auctions. AOL's acquisition of Time-Warner was the largest merger in history when it took place and shows the enormous growth of Internet business! The stock market has had a rocky ride, swooping up and down as the new technology companies, the dot.com's encountered good news and bad. The decline in advertising income spelled doom for many dot.coms, and a major shakeout and search for better business models took place by the survivors.

A current trend with major implications for the future is the growth of high speed connections. 56K modems and the providers who supported them spread widely for a while, but this is the low end now. 56K is not fast enough to carry multimedia, such as sound and video except in low quality. But new technologies many times faster, such as cablemodems and digital subscriber lines (DSL) are predominant now.

Wireless has grown rapidly in the past few years, and travellers search for the wi-fi "hot spots" where they can connect while they are away from the home or office. Many airports, coffee bars, hotels and motels now routinely provide these services, some for a fee and some for free.

A next big growth area is the surge towards universal wireless access, where almost everywhere is a "hot spot". Municipal wi-fi or city-wide access, wiMAX offering broader ranges than wi-fi, EV-DO, 4g, LTE, and other formats will joust for dominance in the USA in the years ahead. The battle is both economic and political.

Another trend that is rapidly affecting web designers is the growth of smaller devices to connect to the Internet. Small tablets, pocket PCs, smart phones, ebooks, game machines, and even GPS devices are now capable of tapping into the web on the go, and many web pages are not designed to work on that scale.

As the Internet has become ubiquitous, faster, and increasingly accessible to non-technical communities, social networking and collaborative services have grown rapidly, enabling people to communicate and share interests in many more ways. Sites like Facebook, Twitter, Linked-In,

YouTube, Flickr, Second Life, delicious, blogs, wikis, and many more let people of all ages rapidly share their interests of the moment with others everywhere.

### 1.3 HOW INTERNET WORKS?

The Internet is a network of networks—millions of them, actually. If the network at your university, your employer, or in your home has Internet access, it connects to an Internet service provider (ISP). Many (but not all) ISPs are big telecommunications companies like Verizon, Comcast, and AT&T<sup>2</sup>. These providers connect to one another, exchanging traffic, and ensuring your messages can get to any other computer that's online and willing to communicate with you. The Internet has no center and no one owns it. That's a good thing. The Internet was designed to be redundant and fault-tolerant—meaning that if one network, connecting wire, or server stops working, everything else should keep on running. Rising from military research and work at educational institutions dating as far back as the 1960s, the Internet really took off in the 1990s, when graphical Web browsing was invented, and much of the Internet's operating infrastructure was transitioned to be supported by private firms rather than government grants.

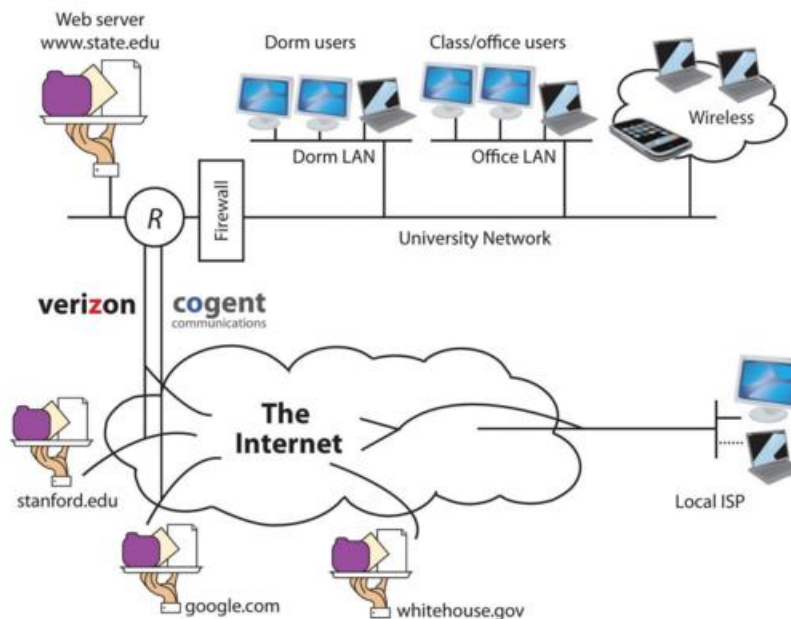


Figure 1: Working of the Internet

Enough history—let's see how it all works! If you want to communicate with another computer on the Internet then your computer needs to know the answer to three questions: What are you looking for? Where is it? And how do we get there? The computers and software that make up Internet infrastructure can help provide the answers. Let's look at how it all comes together.

<sup>2</sup> <http://2012books.lardbucket.org/books/getting-the-most-out-of-information-systems-v1.3/s16-02-internet-101-understanding-how.html>

When you type an address into a Web browser (sometimes called a URL for uniform resource locator), you're telling your browser what you're looking for, Figure 2 describes how to read a typical URL.

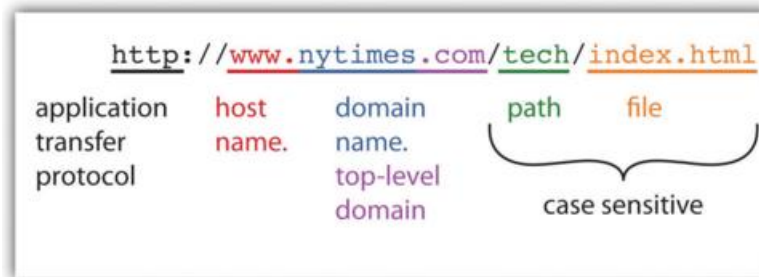


Figure 2: Anatomy of a Web Address

The `http://` you see at the start of most Web addresses stands for hypertext transfer protocol. A protocol is a set of rules for communication—sort of like grammar and vocabulary in a language like English. The `http` protocol defines how Web browser and Web servers communicate and is designed to be independent from the computer's hardware and operating system. It doesn't matter if messages come from a PC, a Mac, a huge mainframe, or a pocket-sized smartphone; if a device speaks to another using a common protocol, then it will be heard and understood.

The Internet supports lots of different applications, and many of these applications use their own application transfer protocol to communicate with each other. The server that holds your e-mail uses something called SMTP, or simple mail transfer protocol, to exchange mail with other e-mail servers throughout the world. FTP, or file transfer protocol, is used for—you guessed it—file transfer. FTP is how most Web developers upload the Web pages, graphics, and other files for their Web sites. Even the Web uses different protocols. When you surf to an online bank or when you're ready to enter your payment information at the Web site of an Internet retailer, the `http` at the beginning of your URL will probably change to `https` (the "s" is for secure). That means that communications between your browser and server will be encrypted for safe transmission. The beauty of the Internet infrastructure is that any savvy entrepreneur can create a new application that rides on top of the Internet.

### 1.3.1 Hosts and Domain Names

The next part of the URL in our diagram holds the host and domain name. Think of the domain name as the name of the network you're trying to connect to, and think of the host as the computer you're looking for on that network.

Many domains have lots of different hosts. For example, Yahoo!'s main Web site is served from the host named "www" (at the address `http://www.yahoo.com`), but Yahoo! also runs other hosts including those named "finance" (`finance.yahoo.com`), "sports" (`sports.yahoo.com`), and "games" (`games.yahoo.com`).



Most Web sites are configured to load a default host, so you can often eliminate the host name if you want to go to the most popular host on a site (the default host is almost always named “www”). Another tip: most browsers will automatically add the “http://” for you, too.

Host and domain names are not case sensitive, so you can use a combination of upper and lower case letters and you’ll still get to your destination.

### **1.3.2 Path Name and File Name**

Look to the right of the top-level domain and you might see a slash followed by either a path name, a file name, or both. If a Web address has a path and file name, the path maps to a folder location where the file is stored on the server; the file is the name of the file you’re looking for.

Most Web pages end in “.html,” indicating they are in hypertext markup language. While http helps browsers and servers communicate, html is the language used to create and format (render) Web pages. A file, however, doesn’t need to be .html; Web servers can deliver just about any type of file: Acrobat documents (.pdf), PowerPoint documents (.ppt or .pptx), Word docs (.doc or .docx), JPEG graphic images (.jpg), and—as we’ll see in Chapter 13 “Information Security: Barbarians at the Gateway (and Just About Everywhere Else)” —even malware programs that attack your PC. At some Web addresses, the file displays content for every visitor, and at others (like amazon.com), a file will contain programs that run on the Web server to generate custom content just for you.

You don’t always type a path or file name as part of a Web address, but there’s always a file lurking behind the scenes. A Web address without a file name will load content from a default page. For example, when you visit “google.com,” Google automatically pulls up a page called “index.html,” a file that contains the Web page that displays the Google logo, the text entry field, the “Google Search” button, and so on. You might not see it, but it’s there.

## ***1.4 ADDRESSING SCHEME IN THE INTERNET***

An Internet Protocol address (IP address) is a numerical label assigned to each device (e.g., computer, printer) participating in a computer network that uses the Internet Protocol for communication<sup>3</sup>. An IP address serves two principal functions: host or network interface identification and location addressing. Its role has been characterized as follows: “A name indicates what we seek. An address indicates where it is. A route indicates how to get there.”

### **1.4.1 IP versions**

Two versions of the Internet Protocol (IP) are in use: IP Version 4 and IP Version 6. Each version defines an IP address differently. Because of its prevalence, the generic term IP address typically still refers to the addresses defined by IPv4. The gap in version sequence between IPv4

---

<sup>3</sup> [https://en.wikipedia.org/wiki/IP\\_address](https://en.wikipedia.org/wiki/IP_address)

and IPv6 resulted from the assignment of number 5 to the experimental Internet Stream Protocol in 1979, which however was never referred to as IPv5.

### 1.4.2 IPv4 Addresses

In IPv4 an address consists of 32 bits which limits the address space to 4294967296 ( $2^{32}$ ) possible unique addresses. IPv4 reserves some addresses for special purposes such as private networks (~18 million addresses) or multicast addresses (~270 million addresses). IPv4 addresses are canonically represented in dot-decimal notation, which consists of four decimal numbers, each ranging from 0 to 255, separated by dots, e.g., 172.16.254.1. Each part represents a group of 8 bits (octet) of the address. In some cases of technical writing, IPv4 addresses may be presented in various hexadecimal, octal, or binary representations.

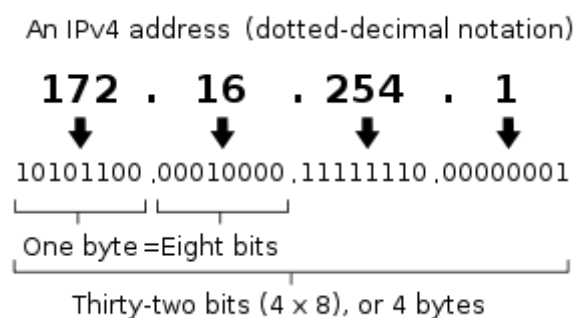


Figure 3: IPv4 address

#### 1.4.2.1 Subnetting

In the early stages of development of the Internet Protocol, network administrators interpreted an IP address in two parts: network number portion and host number portion. The highest order octet (most significant eight bits) in an address was designated as the network number and the remaining bits were called the rest field or host identifier and were used for host numbering within a network.

This early method soon proved inadequate as additional networks developed that were independent of the existing networks already designated by a network number. In 1981, the Internet addressing specification was revised with the introduction of classful network architecture.

Classful network design allowed for a larger number of individual network assignments and fine-grained subnetwork design. The first three bits of the most significant octet of an IP address were defined as the class of the address. Three classes (A, B, and C) were defined for universal unicast addressing. Depending on the class derived, the network identification was based on octet boundary segments of the entire address. Each class used successively additional octets in the network identifier, thus reducing the possible number of hosts in the higher order classes (B and C). The following table gives an overview of this now obsolete system.

Table 1: Historical classful network architecture

Class	Leading bits	Size of network number bit field	Size of rest bit field	Number of networks	Addresses per network	Start address	End address
A	0	8	24	128 ( $2^7$ )	16,777,216 ( $2^{24}$ )	0.0.0.0	127.255.255.255
B	10	16	16	16,384 ( $2^{14}$ )	65,536 ( $2^{16}$ )	128.0.0.0	191.255.255.255
C	110	24	8	2,097,152 ( $2^{21}$ )	256 ( $2^8$ )	192.0.0.0	223.255.255.255

Classful network design served its purpose in the startup stage of the Internet, but it lacked scalability in the face of the rapid expansion of the network in the 1990s. The class system of the address space was replaced with Classless Inter-Domain Routing (CIDR) in 1993. CIDR is based on variable-length subnet masking (VLSM) to allow allocation and routing based on arbitrary-length prefixes. Today, remnants of classful network concepts function only in a limited scope as the default configuration parameters of some network software and hardware components (e.g. netmask), and in the technical jargon used in network administrators' discussions.

#### 1.4.2.2 Private Addresses

Early network design, when global end-to-end connectivity was envisioned for communications with all Internet hosts, intended that IP addresses be uniquely assigned to a particular computer or device. However, it was found that this was not always necessary as private networks developed and public address space needed to be conserved.

Computers not connected to the Internet, such as factory machines that communicate only with each other via TCP/IP, need not have globally unique IP addresses. Three non-overlapping ranges of IPv4 addresses for private networks were reserved in RFC 1918. These addresses are not routed on the Internet and thus their use need not be coordinated with an IP address registry. Today, when needed, such private networks typically connect to the Internet through network address translation (NAT). The designers of the Internet Protocol defined an IP address as a 32-bit number and this system, known as Internet Protocol Version 4 (IPv4), is still in use today. However, because of the growth of the Internet and the predicted depletion of available addresses, a new version of IP (IPv6), using 128 bits for the address, was developed in 1995. IPv6 was standardized as RFC 2460 in 1998, and its deployment has been ongoing since the mid-2000s. IP addresses are usually written and displayed in human-readable notations, such as 172.16.254.1 (IPv4), and 2001:db8:0:1234:0:567:8:1 (IPv6). The Internet Assigned Numbers Authority (IANA) manages the IP address space allocations globally and delegates five regional Internet registries (RIRs) to allocate IP address blocks to local Internet registries (Internet service providers) and other entities.

Table 2: IANA-reserved private IPv4 network ranges

	Start	End	No. of addresses
24-bit block (/8 prefix, 1 × A)	10.0.0.0	10.255.255.255	16 777 216
20-bit block (/12 prefix, 16 × B)	172.16.0.0	172.31.255.255	1 048 576
16-bit block (/16 prefix, 256 × C)	192.168.0.0	192.168.255.255	65 536

Any user may use any of the reserved blocks. Typically, a network administrator will divide a block into subnets; for example, many home routers automatically use a default address range of 192.168.0.0 through 192.168.0.255 (192.168.0.0/24).

### 1.4.2.3 IPv4 address exhaustion

High levels of demand have decreased the supply of unallocated Internet Protocol Version 4 (IPv4) addresses available for assignment to Internet service providers and end user organizations since the 1980s. This development is referred to as IPv4 address exhaustion. IANA's primary address pool was exhausted on 3 February 2011, when the last five blocks were allocated to the five RIRs. APNIC was the first RIR to exhaust its regional pool on 15 April 2011, except for a small amount of address space reserved for the transition to IPv6, intended to be allocated in a restricted process.

### 1.4.3 IPv6 Addresses

The rapid exhaustion of IPv4 address space prompted the Internet Engineering Task Force (IETF) to explore new technologies to expand the addressing capability in the Internet. The permanent solution was deemed to be a redesign of the Internet Protocol itself. This new generation of the Internet Protocol was eventually named Internet Protocol Version 6 (IPv6) in 1995. The address size was increased from 32 to 128 bits (16 octets), thus providing up to  $2^{128}$  (approximately  $3.403 \times 10^{38}$ ) addresses. This is deemed sufficient for the foreseeable future.

The intent of the new design was not to provide just a sufficient quantity of addresses, but also redesign routing in the Internet by more efficient aggregation of subnetwork routing prefixes. This resulted in slower growth of routing tables in routers. The smallest possible individual allocation is a subnet for 264 hosts, which is the square of the size of the entire IPv4 Internet. At these levels, actual address utilization rates will be small on any IPv6 network segment. The new design also provides the opportunity to separate the addressing infrastructure of a network segment, i.e. the local administration of the segment's available space, from the addressing prefix used to route traffic to and from external networks. IPv6 has facilities that automatically change the routing prefix of entire networks, should the global connectivity or the routing policy change, without requiring internal redesign or manual renumbering. The large number of IPv6 addresses allows large blocks to be assigned for specific purposes and, where appropriate, to be aggregated for efficient routing. With a large address space, there is no need to have complex address conservation methods as used in CIDR.



The term subnet mask is only used within IPv4. Both IP versions however use the CIDR concept and notation. In this, the IP address is followed by a slash and the number (in decimal) of bits used for the network part, also called the routing prefix. For example, an IPv4 address and its subnet mask may be 192.0.2.1 and 255.255.255.0, respectively. The CIDR notation for the same IP address and subnet is 192.0.2.1/24, because the first 24 bits of the IP address indicate the network and subnet.

### **1.4.5 IP address assignment**

Internet Protocol addresses are assigned to a host either anew at the time of booting, or permanently by fixed configuration of its hardware or software. Persistent configuration is also known as using a static IP address. In contrast, in situations when the computer's IP address is assigned newly each time, this is known as using a dynamic IP address.

#### **1.4.5.1 Methods**

Static IP addresses are manually assigned to a computer by an administrator. The exact procedure varies according to platform. This contrasts with dynamic IP addresses, which are assigned either by the computer interface or host software itself, as in Zeroconf, or assigned by a server using Dynamic Host Configuration Protocol (DHCP). Even though IP addresses assigned using DHCP may stay the same for long periods of time, they can generally change. In some cases, a network administrator may implement dynamically assigned static IP addresses. In this case, a DHCP server is used, but it is specifically configured to always assign the same IP address to a particular computer. This allows static IP addresses to be configured centrally, without having to specifically configure each computer on the network in a manual procedure.

In the absence or failure of static or stateful (DHCP) address configurations, an operating system may assign an IP address to a network interface using state-less auto-configuration methods, such as Zeroconf.

#### **1.4.5.2 Uses of dynamic address assignment**

IP addresses are most frequently assigned dynamically on LANs and broadband networks by the Dynamic Host Configuration Protocol (DHCP). They are used because it avoids the administrative burden of assigning specific static addresses to each device on a network. It also allows many devices to share limited address space on a network if only some of them will be online at a particular time. In most current desktop operating systems, dynamic IP configuration is enabled by default so that a user does not need to manually enter any settings to connect to a network with a DHCP server. DHCP is not the only technology used to assign IP addresses dynamically. Dialup and some broadband networks use dynamic address features of the Point-to-Point Protocol.

##### *1.4.5.2.1 Sticky dynamic IP address*

A sticky dynamic IP address is an informal term used by cable and DSL Internet access subscribers to describe a dynamically assigned IP address which seldom changes. The addresses are usually assigned with DHCP. Since the modems are usually powered on for extended periods

of time, the address leases are usually set to long periods and simply renewed. If a modem is turned off and powered up again before the next expiration of the address lease, it will most likely receive the same IP address.

### **1.4.5.3 Address autoconfiguration**

RFC 3330 defines an address block, 169.254.0.0/16, for the special use in link-local addressing for IPv4 networks. In IPv6, every interface, whether using static or dynamic address assignments, also receives a local-link address automatically in the block fe80::/10.

These addresses are only valid on the link, such as a local network segment or point-to-point connection, that a host is connected to. These addresses are not routable and like private addresses cannot be the source or destination of packets traversing the Internet.

When the link-local IPv4 address block was reserved, no standards existed for mechanisms of address autoconfiguration. Filling the void, Microsoft created an implementation that is called Automatic Private IP Addressing (APIPA). APIPA has been deployed on millions of machines and has, thus, become a de facto standard in the industry. In RFC 3927, the IETF defined a formal standard for this functionality, entitled Dynamic Configuration of IPv4 Link-Local Addresses.

### **1.4.5.4 Uses of static addressing**

Some infrastructure situations have to use static addressing, such as when finding the Domain Name System (DNS) host that will translate domain names to IP addresses. Static addresses are also convenient, but not absolutely necessary, to locate servers inside an enterprise. An address obtained from a DNS server comes with a time to live, or caching time, after which it should be looked up to confirm that it has not changed. Even static IP addresses do change as a result of network administration (RFC 2072).

### **1.4.5.5 Conflict**

An IP address conflict occurs when two devices on the same local physical or wireless network claim to have the same IP address - that is, they conflict with each other. Since only one of the devices is supposed to be on the network at a time, the second one to arrive will generally stop the IP functionality of one or both of the devices. In many cases with modern Operating Systems, the Operating System will notify the user of one of the devices that there is an IP address conflict (displaying the symptom error message) and then either stop functioning on the network or function very badly on the network, and the user will then be stumped as to how to resolve the conflict, probably considering the situation an emergency. In some unfortunate cases, both devices will function very badly on the network. In severe cases in which one of the devices is the gateway, the network will be crippled. Since IP addresses are assigned by multiple people and systems in multiple ways, any of them can be at fault.

## **1.4.6 Routing**

IP addresses are classified into several classes of operational characteristics: unicast, multicast, anycast and broadcast addressing.

### **1.4.6.1 Unicast addressing**

The most common concept of an IP address is in unicast addressing, available in both IPv4 and IPv6. It normally refers to a single sender or a single receiver, and can be used for both sending and receiving. Usually, a unicast address is associated with a single device or host, but a device or host may have more than one unicast address. Some individual PCs have several distinct unicast addresses, each for its own distinct purpose. Sending the same data to multiple unicast addresses requires the sender to send all the data many times over, once for each recipient.

### **1.4.6.2 Broadcast addressing**

In IPv4 it is possible to send data to all possible destinations ("all-hosts broadcast"), which permits the sender to send the data only once, and all receivers receive a copy of it. In the IPv4 protocol, the address 255.255.255.255 is used for local broadcast. In addition, a directed (limited) broadcast can be made by combining the network prefix with a host suffix composed entirely of binary 1s. For example, the destination address used for a directed broadcast to devices on the 192.0.2.0/24 network is 192.0.2.255. IPv6 does not implement broadcast addressing and replaces it with multicast to the specially-defined all-nodes multicast address.

### **1.4.6.3 Multicast addressing**

A multicast address is associated with a group of interested receivers. In IPv4, addresses 224.0.0.0 through 239.255.255.255 (the former Class D addresses) are designated as multicast addresses. IPv6 uses the address block with the prefix ff00::/8 for multicast applications. In either case, the sender sends a single datagram from its unicast address to the multicast group address and the intermediary routers take care of making copies and sending them to all receivers that have joined the corresponding multicast group.

### **1.4.6.4 Anycast addressing**

Like broadcast and multicast, anycast is a one-to-many routing topology. However, the data stream is not transmitted to all receivers, just the one which the router decides is logically closest in the network. Anycast address is an inherent feature of only IPv6. In IPv4, anycast addressing implementations typically operate using the shortest-path metric of BGP routing and do not take into account congestion or other attributes of the path. Anycast methods are useful for global load balancing and are commonly used in distributed DNS systems.

## **1.4.7 Public addresses**

A public IP address, in common parlance, is synonymous with a globally routable unicast IP address. Both IPv4 and IPv6 define address ranges that are reserved for private networks and link-local addressing. The term public IP address often used excludes these types of addresses.

## **1.4.8 Modifications to IP addressing**

### **1.4.8.1 IP blocking and firewalls**

Firewalls perform Internet Protocol blocking to protect networks from unauthorized access. They are common on today's Internet. They control access to networks based on the IP address of a client computer. Whether using a blacklist or a whitelist, the IP address that is blocked is the



perceived IP address of the client, meaning that if the client is using a proxy server or network address translation, blocking one IP address may block many individual computers.

### 1.4.8.2 IP address translation

Multiple client devices can appear to share IP addresses: either because they are part of a shared hosting web server environment or because an IPv4 network address translator (NAT) or proxy server acts as an intermediary agent on behalf of its customers, in which case the real originating IP addresses might be hidden from the server receiving a request. A common practice is to have a NAT hide a large number of IP addresses in a private network. Only the "outside" interface(s) of the NAT need to have Internet-routable addresses.

Most commonly, the NAT device maps TCP or UDP port numbers on the side of the larger, public network to individual private addresses on the masqueraded network. In small home networks, NAT functions are usually implemented in a residential gateway device, typically one marketed as a "router". In this scenario, the computers connected to the router would have private IP addresses and the router would have a public address to communicate on the Internet. This type of router allows several computers to share one public IP address.

## 1.5 INTERNET SERVICE PROVIDER

An Internet service provider (ISP) is an organization that provides services for accessing, using, or participating in the Internet<sup>5</sup>. Internet service providers may be organized in various forms, such as commercial, community-owned, non-profit, or otherwise privately owned. Internet services typically provided by ISPs include Internet access, Internet transit, domain name registration, web hosting, Usenet service, and collocation.

### 1.5.1 Classification of ISP<sup>6</sup>

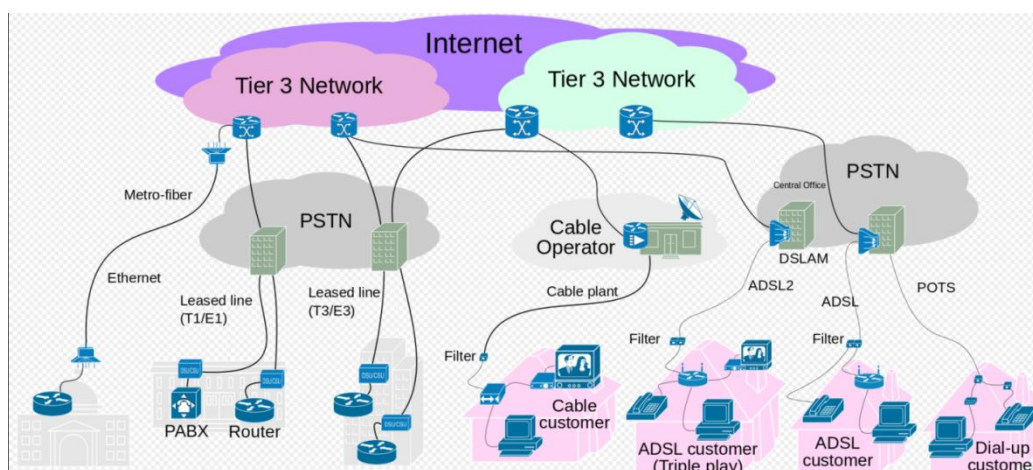


Figure 5: Internet connectivity options from end-user to tier 3/2 ISPs

<sup>5</sup> [https://en.wikipedia.org/wiki/Internet\\_service\\_provider](https://en.wikipedia.org/wiki/Internet_service_provider)

<sup>6</sup> [https://en.wikipedia.org/wiki/Internet\\_service\\_provider](https://en.wikipedia.org/wiki/Internet_service_provider)

### **1.5.1.1 Access providers ISP**

ISPs provide Internet access, employing a range of technologies to connect users to their network. Available technologies have ranged from computer modems with acoustic couplers to telephone lines, to television cable (CATV), wireless Ethernet (wi-fi), and fiber optics.

For users and small businesses, traditional options include copper wires to provide dial-up, DSL (typically asymmetric digital subscriber line (ADSL), cable modem or Integrated Services Digital Network (ISDN) (typically basic rate interface). Using fiber-optics to end users is called Fiber To The Home or similar names. For customers with more demanding requirements (such as medium-to-large businesses, or other ISPs) can use higher-speed DSL (such as single-pair high-speed digital subscriber line), Ethernet, metropolitan Ethernet, gigabit Ethernet, Frame Relay, ISDN Primary Rate Interface, ATM (Asynchronous Transfer Mode) and synchronous optical networking (SONET). Wireless access is another option, including satellite Internet access.

### **1.5.1.2 Mailbox providers**

A mailbox provider is an organization that provides services for hosting electronic mail domains with access to storage for mail boxes. It provides email servers to send, receive, accept, and store email for end users or other organizations. Many mailbox providers are also access providers, while others are not (e.g., Yahoo! Mail, Outlook.com, Gmail, AOL Mail, Po box). The definition given in RFC 6650 covers email hosting services, as well as the relevant department of companies, universities, organizations, groups, and individuals that manage their mail servers themselves. The task is typically accomplished by implementing Simple Mail Transfer Protocol (SMTP) and possibly providing access to messages through Internet Message Access Protocol (IMAP), the Post Office Protocol, Webmail, or a proprietary protocol.

### **1.5.1.3 Hosting ISPs**

Internet hosting services provide email, web-hosting, or online storage services. Other services include virtual server, cloud services, or physical server operation.

### **1.5.1.4 Transit ISP**

Just as their customers pay them for Internet access, ISPs themselves pay upstream ISPs for Internet access. An upstream ISP usually has a larger network than the contracting ISP or is able to provide the contracting ISP with access to parts of the Internet the contracting ISP by itself has no access to. In the simplest case, a single connection is established to an upstream ISP and is used to transmit data to or from areas of the Internet beyond the home network; this mode of interconnection is often cascaded multiple times until reaching a tier 1 carrier. In reality, the situation is often more complex. ISPs with more than one point of presence (PoP) may have separate connections to an upstream ISP at multiple PoPs, or they may be customers of multiple upstream ISPs and may have connections to each one of them at one or more point of presence. Transit ISPs provide large amounts of bandwidth for connecting hosting ISPs and access ISPs.

### **1.5.1.5 Virtual ISPs**

A virtual ISP (VISP) is an operation that purchases services from another ISP, sometimes called a wholesale ISP in this context, which allow the VISP's customers to access the Internet using services and infrastructure owned and operated by the wholesale ISP. VISPs resemble mobile virtual network operators and competitive local exchange carriers for voice communications.

### **1.5.1.6 Free ISPs**

Free ISPs are Internet service providers that provide service free of charge. Many free ISPs display advertisements while the user is connected; like commercial television, in a sense they are selling the user's attention to the advertiser. Other free ISPs, sometimes called freenets, are run on a nonprofit basis, usually with volunteer staff.

### **1.5.1.7 Wireless ISP**

A wireless internet service provider (WISP) is an Internet service provider with a network based on wireless networking. Technology may include commonplace Wi-Fi wireless mesh networking, or proprietary equipment designed to operate over open 900 MHz, 2.4 GHz, 4.9, 5.2, 5.4, 5.7, and 5.8 GHz bands or licensed frequencies such as 2.5 GHz (EBS/BRS), 3.65 GHz (NN) and in the UHF band (including the MMDS frequency band) and LMDS.

## ***1.6 DOMAIN NAME SYSTEM(DNS)***

The Domain Name System (DNS) is the system used to translate alphanumeric domain names into Internet Protocol numbers. Simply put, the DNS converts the names typed in the Web browser address bar into IP addresses<sup>7</sup>. The DNS is made up of many servers and databases which, through a series of lookups in various caches, configure Domain Names into IP Addresses. The Domain Name System is a distributed database arranged hierarchically; its purpose is to provide a layer of abstraction between Internet services (web, email, etc.) and the numeric addresses (IP addresses) used to uniquely identify any given machine on the Internet. The DNS associates a variety of information with the domain names assigned and, most importantly, translates the domain names meaningful to humans into the numerical identifiers that locate the desired destination.

### **1.6.1 How does it work?**

The DNS makes it possible to assign domain names in a meaningful way to Internet resources as well as to users, regardless of the entity's location. As a result, the WWW hyperlinks remain consistent, even for mobile devices. A domain name is an easy way to remember an address, but that needs to be converted to its numerical, IP format.

Coordination across the Internet is maintained by means of a complex authoritative root system known as the Top Level Domain (TLD), as well as the DNS and other smaller name servers responsible for hosting individual domain information.

---

<sup>7</sup> [http://icannwiki.com/Domain\\_Name\\_System](http://icannwiki.com/Domain_Name_System)

DNS includes three types of top-level domains: generic (gTLD), country code (ccTLD), and sponsored (sTLD). gTLDs include domains that could be obtained by anyone (.com, .info, .net, and .org). Since 2014 many other gTLDs have been added like .pub, .ngo, .sucks. sTLDs are limited to a specific group e.g .aero (for air-transport industry).

For each domain, the DNS spreads the responsibility by mapping the domain names and assigning them into IP addresses, and vice-versa. This is accomplished through authoritative name servers which have been designated for each domain. Each authoritative name server is responsible for its own particular domain, but it has the authority to assign new authoritative name servers to any of its sub-domains. The DNS is able to store many types of information, even the mail server lists for a specific domain. The DNS is a core element which ensures the functionality of the Internet through its distributed keyword-based redirection service.

However, the DNS does not include security extensions, which was instead developed as DNSSEC.

### 1.6.1.1 Top-Level Domain(TLD)<sup>8</sup>

Whenever you use a domain name, in a web address(URL), email address, or wherever, it *ends* in a "top-level domain" or "TLD". This is the last part of the name. We often think of .COM, .ORG, .NET, etc., as in:

- www.disruptiveconversations.COM
- www.forimmediaterelease.BIZ
- internetsociety.ORG

TLDs are broadly classified into two categories:

- a. generic top-level domains (gTLDs)
- b. country code top-level domains (ccTLDs)

The entity responsible for the administration of these TLDs in the "root" of the Domain Name System (DNS) is the Internet Assigned Numbers Authority (IANA) that is currently operated by the Internet Corporation for Assigned Names and Numbers (ICANN). You can see the full list of current TLDs at: <https://www.iana.org/domains/root/db>

### 1.6.1.2 Second-Level Domain

The next part of the domain name to the left of the TLD (and separated by a dot) is the "second-level domain". These are the domains that you are typically able to register with a registrar. Examples include:

- www.disruptiveconversations.com
- www.forimmediaterelease.biz
- internetsociety.org

The next part of the domain name to the left ("www" in the first two examples above) would be called the "third-level domain", and so on.

---

<sup>8</sup> <http://www.disruptiveconversations.com/2014/03/what-is-a-tld-gtld-ccTld-newgtld-idn.html>

- a. **gTLD (Generic Top-Level Domain):** Generic top-level domains (gTLDs) are TLDs that are not tied to any specific country and are "generic" in terms of being able to be used (in theory, anyway) by anyone on the Internet anywhere in the world. The "original" TLDs such as .COM, .ORG, .NET, .GOV, .MIL are all classified as "generic TLDs". There were a couple of rounds of "expansion" of the gTLDs that brought the total to 22 gTLDs prior to the "newgTLD" expansion currently underway
- b. **ccTLD (Country Code Top-Level Domain):** Country code top-level domains(ccTLDs) are *two letter TLDs* that are assigned to *countries* based mostly on the ISOC 3166 list of country codes. Some countries have chosen to operate their ccTLD exclusively for domains within their country or geographic territory. Some do not allow people to register "second-level domains" under the TLD and instead require people to register third-level domains under one of several different second-level domains. For example, the .UK domain as to date required registrations to be under domains such as ".co.uk" and ".org.uk", basically duplicating part of the original gTLD scheme inside their ccTLD.  
Many ccTLDs have chosen **NOT** to restrict their ccTLD to people in their country and have in fact marketed their domains very widely encouraging everyone to use them. Some prominent examples of this include Columbia(.CO), Montenegro(.ME), Tuvulu(.TV), Federated States of Micronesia(.FM) and many more. Essentially, any time you are using a two-letter TLD, it is a ccTLD for some country.
- c. **newgTLD Top-Level Domain:** After many years of discussion, ICANN's board voted in 2011 to allow the creation of new generic TLDs using almost any text string (and in multiple character sets) and began the "newgTLD" program. This resulted in 1,930 applications by various companies to operate new gTLDs. These newgTLDs are now being rolled out in phases and people are able to register second-level domains under many of these domains. More newgTLDs are being made available pretty much every week - and the expansion will continue for many months and years ahead of us.  
At a technical level, "new gTLDs" are effectively the same as "gTLDs"... the designation is just really that these new gTLDs are coming out in this current round of expansion.
- d. **IDN = Internationalized Domain Name:** The original TLDs were all in the ASCII character set, but over time ICANN decided to allow the creation of "internationalized domain names"(IDNs) that use other character sets such as Cyrillic, Arabic, Chinese, Korean, etc. The first IDN for a country code TLD appeared in 2010 and the newgTLDs contain many IDNs. (In fact, the very first of the "newgTLDs" were four IDNs.)

## ***1.7 WORLD WIDE WEB(WWW)***

The World Wide Web, is a system of interlinked hypertext documents accessed via the Internet. With a web browser, one can view web pages that may contain text, images, videos, and other multimedia, and navigate between them via hyperlinks. Using concepts from his earlier hypertext systems like ENQUIRE, British engineer, computer scientist and at that time employee of

CERN, Sir Tim Berners-Lee, now Director of the World Wide Web Consortium, wrote a proposal in March 1989 for what would eventually become the World Wide Web<sup>9</sup>.

### **1.7.1 Is Internet and www similar?**

The world wide web is just one way to access information through the internet<sup>10</sup>. While it does represent a considerable portion of the internet, and is unquestionably the most popular part, the two concepts must not be treated as synonyms because they are not the same. We tend to become used to calling things by the simplest possible name but we also tend to muddle concepts and mix up one thing with another when the distinction between them isn't very clear. One very common case of this is the fact that most people tend to refer to "the web" and "internet" as if they were exactly the same thing, when in fact they're not. It can be rather confusing, and even a surprise for many, but the internet and the web are two different things, and one is above the other. Let's see what this means.

#### **1.7.1.1 The www**

The three Ws that are in the addresses of the websites we access. The world wide web or simply the "web", is a way to access information through the internet. The web is a model for sharing information that is built on the internet. The protocol used by the web is HTTP, just one of the many ways that information can be sent through the internet.

If a service uses HTTP to enable applications to communicate with each other, this is a web service. Web browsers, such as Chrome or Firefox, enable us to access web documents that we mainly know as web pages or websites. These sites are connected to each other through hyperlinks as if they were on a spider's web (hence the name), and all this thanks to the transfer protocol: HTTP.

Therefore, the web is only one of the ways that information can flow through the internet: it is just a portion, and although it is very large and the most popular part, it does not include the whole of the internet.

#### **1.7.1.2 The Internet**

The internet is a massive network, the network of networks. The internet connects millions of computers across the globe through a network that enables any computer to be able to communicate with another, no matter where on the planet they are, provided they are both connected to the internet. A network is any connection between two or more clients. For example, you can access a local network in your home that only the computers of the members of your family can access and which are connected through a switcher or router, or a work network that only people working at the same firm can access. The internet is a global, large-scale network that enables millions and millions of devices to connect at the same time, and is completely free and open.

All the information that travels through the internet does so through a protocol; there are several of these. As we have already explained, the HTTP protocol is the one used by the web to share

---

<sup>9</sup> <http://jobs.code4lib.org/jobs/world-wide-web/>

<sup>10</sup> <http://blogthinkbig.com/internet-and-the-world-wide-web/>

information. Therefore, web pages such as Twitter, Google, Facebook and even this blog are part of the web and this information travels to us all through the internet.

When it comes down to it, the world won't end if we continue using the terms interchangeably – after all, habits are hard to break – but it is a good thing to be clear about the concepts, at least.

## ***1.8 APPLICATION OF INTERNET***

Internet have become an essential component of our daily lives. But what does one do with the Internet? May be four things, basically: mail, discussion groups, long-distance computing, and file transfers. Internet mail is (e-mail or electronic mail), much faster as compared to normal postal mail<sup>11</sup>. One can also send software and certain forms of compressed digital image as an attachment. News groups or discussion groups facilitate Internet user to join for various kinds of debate, discussion and news sharing. Long-distance computing was an original inspiration for development of ARPANET and does still provide a very useful service on Internet. Programmers can maintain accounts on distant, powerful computers, execute programs. File transfer service allows Internet users to access remote machines and retrieve programs, data or text.

We can roughly separate internet applications into the following types: online media, online information search, online communications, online communities, online entertainment, e-business, online finance and other applications. The internet is treated as one of the biggest invention. It has a large number of uses.

1. Communication
2. Job searches
3. Finding books and study material
4. Health and medicine
5. Travel
6. Entertainment
7. Shopping
8. Stock market updates
9. Research
10. Business use of internet: different ways by which internet can be used for business are:
  - a. Information about the product can be provided online to the customer .
  - b. Provide market information to the business
  - c. It help business to recruit talented people
  - d. Help in locating suppliers of the product
  - e. Fast information regarding customers view about companies product
  - f. Eliminate middle men and have a direct contact with customer
  - g. Providing information to the investor by providing companies back ground and financial information on web site.

---

<sup>11</sup> [http://oer.nios.ac.in/wiki/oer/ictapplication/internetanditsusage/internet\\_applications\\_and\\_services.html](http://oer.nios.ac.in/wiki/oer/ictapplication/internetanditsusage/internet_applications_and_services.html)

## 1.9 SUMMARY

1. J.C.R. Licklider of MIT first proposed a global network of computers in 1962, and moved over to the Defense Advanced Research Projects Agency (DARPA) in late 1962 to head the work to develop it.
2. Leonard Kleinrock of MIT and later UCLA developed the theory of packet switching, which was to form the basis of Internet connections.
3. The Internet, also known as ARPANET, was brought online in 1969 under a contract let by the renamed Advanced Research Projects Agency (ARPA) which initially connected four major computers at universities in the southwestern US (UCLA, Stanford Research Institute, UCSB, and the University of Utah).
4. The Internet was designed to provide a communications network that would work even if some of the major sites were down.
5. E-mail was adapted for ARPANET by Ray Tomlinson of BBN in 1972.
6. In 1986, the National Science Foundation funded NSFNet as a cross country 56 Kbps backbone for the Internet. They maintained their sponsorship for nearly a decade, setting rules for its non-commercial government and research uses.
7. The first effort, other than library catalogs, to index the Internet was created in 1989, as Peter Deutsch and Alan Emtage, students at McGill University in Montreal, created an archiver for ftp sites, which they named Archie.
8. Tim Berners-Lee and others at the European Laboratory for Particle Physics, more popularly known as CERN, proposed a new protocol for information distribution. This protocol, which became the World Wide Web in 1991, was based on hypertext--a system of embedding links in text to link to other text, which you have been using every time you selected a text link while reading these pages.
9. Marc AndreessenThe development in 1993 of the graphical browser Mosaic by Marc Andreessen and his team at the National Center For Supercomputing Applications (NCSA) gave the protocol its big boost.
10. Since the Internet was initially funded by the government, it was originally limited to research, education, and government uses.
11. Commercial uses were prohibited unless they directly served the goals of research and education. This policy continued until the early 90's, when independent commercial networks began to grow. It then became possible to route traffic across the country from one commercial site to another without passing through the government funded NSFNet Internet backbone.
12. The Internet has no center and no one owns it.
13. The Internet supports lots of different applications, and many of these applications use their own application transfer protocol to communicate with each other.
14. Host and domain names are not case sensitive, so you can use a combination of upper and lower case letters and you'll still get to your destination.



15. An Internet Protocol address (IP address) is a numerical label assigned to each device (e.g., computer, printer) participating in a computer network that uses the Internet Protocol for communication.
16. An IP address serves two principal functions: host or network interface identification and location addressing.
17. Two versions of the Internet Protocol (IP) are in use: IP Version 4 and IP Version 6.
18. The Domain Name System (DNS) is the system used to translate alphanumeric domain names into Internet Protocol numbers.
19. The World Wide Web, is a system of interlinked hypertext documents accessed via the Internet.
20. The world wide web or simply the “web”, is a way to access information through the internet.

### ***1.10 CHECK YOUR PROGRESS***

1. DARPA stands for \_\_\_\_\_.
2. The Unix to Unix Copy Protocol (UUCP) was invented in \_\_\_\_\_ at Bell Labs.
3. VERONICA stands for \_\_\_\_\_.
4. \_\_\_\_\_ was the first national commercial online service to offer Internet access to its subscribers.
5. WAIS stands for \_\_\_\_\_.
6. SMTP stands for \_\_\_\_\_.
7. An \_\_\_\_\_ is an organization that provides services for accessing, using, or participating in the Internet.
8. DNS converts the names typed in the Web browser address bar into \_\_\_\_\_.

### ***1.11 ANSWERS TO CHECK YOUR PROGRESS***

1. Defense Advanced Research Projects Agency
2. 1978
3. Very Easy Rodent-Oriented Netwide Index to Computerized Archives
4. Delphi
5. Wide Area Information Server
6. simple mail transfer protocol
7. Internet service provider
8. IP addresses

### ***1.12 MODEL QUESTIONS***

1. Describe the brief history of Internet.
2. What is ARPANET?
3. Name the four Universities which were initially connected by ARPANET.
4. Who were the first to propose TCP/IP architecture?
5. What is Archie?
6. What is http?

7. What do you mean by redundant and fault-tolerant design?
8. What is URL?
9. How http:// is different from https:// ?
10. What is an IP address? Explain the addressing scheme in the Internet.
11. What is subnetting? Explain.
12. Write a short note on IPv4.
13. What is classful network architecture?
14. What are private addresses?
15. Explain IPv6 addresses.
16. What is a sticky dynamic IP address?
17. Explain unicast, multicast, anycast and broadcast addressing.
18. What is an ISP? Explain different classifications of an ISP.
19. What is a virtual ISP?
20. What is DNS? How does it works?
21. What is the difference between Internet and www?

## UNIT II: MODELS OF E-GOVERNANCE

### 2.1 LEARNING OBJECTIVES

After going through this unit, you will be able to:

- Define E-Governance.
- Understand the goals of e-governance.
- Know the benefits of e-governance.
- Understand the different stages of e-governance.
- Differentiate between various models of e-governance.
- Understand legal and policy framework for facilitating ICT in e-governance.
- Understand e-governance maturity models.

### 2.2 E-GOVERNANCE

Electronic governance<sup>12</sup> or e-governance is the application of information and communication technology (ICT) for delivering government services, exchange of information communication transactions, integration of various stand-alone systems and services between government-to-customer (G2C), government-to-business (G2B), government-to-government (G2G) as well as back office processes and interactions within the entire government framework. Through e-governance, government services are made available to citizens in a convenient, efficient and transparent manner. The three main target groups that can be distinguished in governance concepts are government, citizens and businesses/interest groups. In e-governance there are no distinct boundaries.

The goals of e-Governance are<sup>13</sup>:

- a. Better service delivery to citizens
- b. Ushering in transparency and accountability
- c. Empowering people through information
- d. Improved efficiency within Governments
- e. Improve interface with business and industry.

#### 2.2.1 Benefits of e-governance

E-Governance is about reform in governance, facilitated by the creative use of Information and Communications Technology. It is expected that this would lead to:

- i. **Better access to information and quality services for citizens:** ICT would make available timely and reliable information on various aspects of governance. In the initial phase, information would be made available with respect to simple aspects of governance such as forms, laws, rules, procedures etc later extending to detailed information including reports (including performance reports), public database, decision making

---

<sup>12</sup> <https://en.wikipedia.org/wiki/E-governance>

<sup>13</sup> [http://arc.gov.in/11threp/ARC\\_11thReport\\_preface\\_contents.pdf](http://arc.gov.in/11threp/ARC_11thReport_preface_contents.pdf)

processes etc. As regards services, there would be an immediate impact in terms of savings in time, effort and money, resulting from online and one-point accessibility of public services backed up by automation of back end processes. The ultimate objective of e-Governance is to reach out to citizens by adopting a life-cycle approach i.e. providing public services to citizens which would be required right from birth to death.

- ii. **Simplicity, efficiency and accountability in the government:** Application of ICT to governance combined with detailed business process reengineering would lead to simplification of complicated processes, weeding out of redundant processes, simplification in structures and changes in statutes and regulations. The end result would be simplification of the functioning of government, enhanced decision making abilities and increased efficiency across government – all contributing to an overall environment of a more accountable government machinery. This, in turn, would result in enhanced productivity and efficiency in all sectors.
- iii. **Expanded reach of governance:** Rapid growth of communications technology and its adoption in governance would help in bringing government machinery to the doorsteps of the citizens. Expansion of telephone network, rapid strides in mobile telephony, spread of internet and strengthening of other communications infrastructure would facilitate delivery of a large number of services provided by the government. This enhancement of the reach of government – both spatial and demographic – would also enable better participation of citizens in the process of governance.

Generally four type of communication in e-governance:

- a. **G2G (Government to Government)**– In this case, Information and Communications Technology is used not only to restructure the governmental processes involved in the functioning of government entities but also to increase the flow of information and services within and between different entities. This kind of interaction is only within the sphere of government and can be both horizontal i.e. between different government agencies as well as between different functional areas within an organisation, or vertical i.e. between national, provincial and local government agencies as well as between different levels within an organisation. The primary objective is to increase efficiency, performance and output.
- b. **G2C (Government to Citizens)** – In this case, an interface is created between the government and citizens which enables the citizens to benefit from efficient delivery of a large range of public services. This expands the availability and accessibility of public services on the one hand and improves the quality of services on the other. It gives citizens the choice of when to interact with the government (e.g. 24 hours a day, 7 days a week), from where to interact with the government (e.g. service centre, unattended kiosk or from one's home/workplace) and how to interact with the government (e.g. through internet, fax, telephone, email, face-to-face, etc). The primary purpose is to make government, citizen-friendly.

- c. **G2B (Government to Business)** – Here, e-Governance tools are used to aid the business community – providers of goods and services – to seamlessly interact with the government. The objective is to cut red tape, save time, reduce operational costs and to create a more transparent business environment when dealing with the government. The G2B initiatives can be transactional, such as in licensing, permits, procurement and revenue collection. They can also be promotional and facilitative, such as in trade, tourism and investment. These measures help to provide a congenial environment to businesses to enable them to perform more efficiently.
- d. **G2E (Government to Employees)** – Government is by far the biggest employer and like any organisation, it has to interact with its employees on a regular basis. This interaction is a two-way process between the organisation and the employee. Use of ICT tools helps in making these interactions fast and efficient on the one hand and increase satisfaction levels of employees on the other.

### 2.2.2 Evolution of e-governance in India

Recognising the increasing importance of electronics, the Government of India established the Department of Electronics in 1970. The subsequent establishment of the National Informatics Centre (NIC) in 1977 was the first major step towards e-Governance in India as it brought 'information' and its communication in focus. In the early 1980s, use of computers was confined to very few organizations. The advent of personal computers brought the storage, retrieval and processing capacities of computers to Government offices. By the late 1980s, a large number of government officers had computers but they were mostly used for 'word processing'. Gradually, with the introduction of better softwares, computers were put to other uses like managing databases and processing information. Advances in communications technology further improved the versatility and reach of computers, and many Government departments started using ICT for a number of applications like tracking movement of papers and files, monitoring of development programmes, processing of employees' pay rolls, generation of reports etc.

However, the main thrust for e-Governance was provided by the launching of NICNET in 1987 – the national satellite-based computer network. This was followed by the launch of the District Information System of the National Informatics Centre (DISNIC) programme to computerize all district offices in the country for which free hardware and software was offered to the State Governments. NICNET was extended via the State capitals to all district headquarters by 1990.

In the ensuing years, with ongoing computerization, teleconnectivity and internet connectivity, came a large number of e-Governance initiatives, both at the Union and State levels. A National Task Force on Information Technology and Software Development was constituted in May 1998. While recognizing Information Technology as a frontier area of knowledge per se, it focused on utilizing it as an enabling tool for assimilating and processing all other spheres of knowledge. It recommended the launching of an 'Operation Knowledge' aimed at universalizing computer literacy and spreading the use of computers and IT in education. In 1999, the Union Ministry of Information Technology was created. By 2000, a 12-point minimum agenda for e-Governance was identified by Government of India for implementation in all the Union

Government Ministries/Departments. The agenda undertaken included the following action points:

- i. Each Ministry/Department must provide PCs with necessary software up to the Section Officer level. In addition, Local Area Network (LAN) must also be set up.
- ii. It should be ensured that all staff who have access to and need to use computer for their office work are provided with adequate training. To facilitate this, inter alia, Ministries/Departments should set up their own or share other's Learning Centres for decentralized training in computers as per the guidelines issued by the MIT.
- iii. Each Ministry/Department should start using the Office Procedure Automation software developed by NIC with a view to keeping a record of receipt of dak, issue of letters, as well as movement of files in the department.
- iv. Pay roll accounting and other house-keeping software should be put to use in day-to-day operations.
- v. Notices for internal meetings should be sent by e-mail. Similarly, submission of applications for leave and for going on tour should also be done electronically. Ministries/Departments should also set up online notice board to display orders, circulars etc. as and when issued.
- vi. Ministries/Departments should use the web-enabled Grievance Redressal Software developed by the Department of Administrative Reforms and Public Grievances.
- vii. Each Ministry/Department should have its own website.
- viii. All Acts, Rules, Circulars must be converted into electronic form and, along with other published material of interest or relevance to the public, should be made available on the internet and be accessible from the Information and Facilitation Counter.
- ix. The websites of Ministries/Departments/Organisations should specifically contain a section in which various forms to be used by citizens/customers are available. The forms should be available for being printed or for being completed on the computer itself and then printed out for submission. Attempts should also be made to enable completion and submission of forms online.
- x. The Hindi version of the content of the websites should as far as possible be developed simultaneously.
- xi. Each Ministry/Department would also make efforts to develop packages so as to begin electronic delivery of services to the public.
- xii. Each Ministry/Department should have an overall IT vision or strategy for a five year period, within which it could dovetail specific action plans and targets (including the minimum agenda) to be implemented within one year.

Many countries have initiated e-Governance programmes in order to make government and its agencies efficient, more responsive and transparent. Some of these initiatives can be found at:

[http://arc.gov.in/11threp/arc\\_11threport\\_ch3.pdf](http://arc.gov.in/11threp/arc_11threport_ch3.pdf)

## ***2.3 AIM OF E-GOVERNANCE***

The complete transformation of the processes of Governance using the implementation of Information & Communication Technology is called E-Governance<sup>14</sup>. It aims at bringing in faster and transparent service delivery, accountability, information sharing and people participation in the decision making and govt. processes.

It brings in SMART Governance viz.:

**S - Simple:** Simplification of rules and procedures of Government making it user-friendly.

**M-Moral:** Infusing ethics and morals into officers again since anti-corruption and vigilance agencies improving.

**A- Accountable:** ICT helps set standards of performance and efficiently measures it.

**R- Responsive:** Efficient service delivery and government that is in tune with the people.

**T- Transparent:** Information confined to secrecy is out in the public domain bringing equity and rule of law in public agencies.

SMART Governance enables:

1. People participation
2. Accountability and efficiency
3. Transparency
4. User friendly government processes
5. Removal of hierarchical barriers and red tape
6. Better service delivery

## ***2.4 STAGES OF E-GOVERNANCE***

1. Simple Information Dissemination - A one way broadcasting of information stage from Govt. to the constituents.
2. Two-Way Communication - A request and response form of communication which is generally done in the manner of emails, website form filling, etc.
3. Online Service Transactions - Citizens can perform a number of online services and financial transactions on a website in a self service form.
4. Integration (Vertical & Horizontal) - Via this method the government attempts inter & intra-governmental integration by means of ICT to remove the hierarchical barriers inducing red-tapism in service delivery and information dissemination.
5. Political Participation - Online voting, online polling, online public forums and wider interaction with the government.

## ***2.5 MODELS OF E-GOVERNANCE<sup>15</sup>***

Digital Governance models keep on expanding and evolving as new applications of ICTs come to light and to deal with new issues in the area of governance. There are no rigid or finite models

---

<sup>14</sup> The unit is thankfully adopted from <http://www.publicadministrationtheone.blogspot.in/2014/02/e-governance-concept-significance.html>

<sup>15</sup> Thankfully adapted from <http://www.digitalgovernance.org/index.php/models> with due permission from the Mr. Vikas Nath, Founder- DigitalGovernance.org

of Digital Governance. In fact developing countries are experimenting on their own to find which models will work for them and will best serve their needs. Some of these models may be technologically simple but are changing the way information is distributed and used in the society. Based on primary experimentation and secondary research, a few generic models which have emerged and are being practiced have been identified.

These Digital Governance models should be examined in light of:

- Emergence of knowledge societies and knowledge networkers
- Role of information in governance process, and
- Link between ICT and governance.

### 2.5.1 Broadcasting Model

Broadcasting model is based on mass dissemination of governance-related information which is already available in the public domain into the wider public domain using ICTs. This raises awareness among the citizens about ongoing governance processes and government services that are available to them and how they can benefit from them. It allows citizens to form an opinion of the government and its administration based on services delivered to them - whether the government services were available to them, and the quality of service received. This could be judged in terms of time spent, number of visits required and level of bureaucracy encountered to avail the services. Equipped with this information, the citizens can feel more empowered to voice their concerns and influence governance processes to make them more efficient. The application of this model using appropriate technologies, could reduce the "information failure situations" where citizens are unaware of new and existing services being provided by the government. It can also provide an alternative channel to people to stay updated of governance related information and to validate information received from other sources.

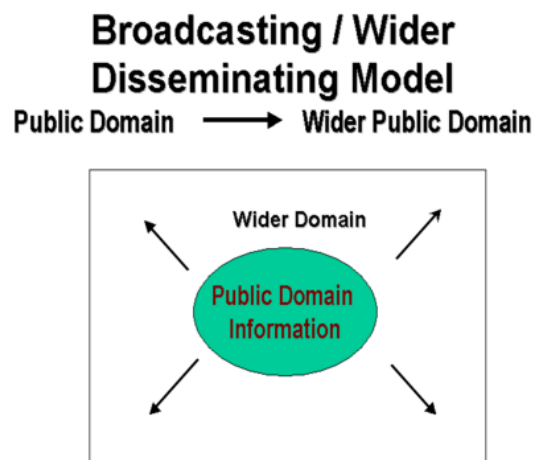


Figure 6: Broadcasting model

#### Applications

- Putting governmental laws and legislations online



- Making available the names, contact addresses, emails, mobile numbers of local/regional/ national government officials online.
- Make available information such as governmental plans, budgets, expenditures, and performance reports online.
- Putting key judicial decisions which are of value to general citizens and create a precedence for future actions online. viz. key environmental decisions, state vs. citizen decisions etc.

The Broadcasting Model is a stepping stone to more complex Digital Governance models. It is also the most fundamental model as it enhances 'access' and 'flow' of information to all segments of the society, which is essential to bringing good governance. In several developing countries, even the basic governance-related information is unavailable, for instance, the opening and closing times of government offices, or information government department and units which deal with specific issues such as agricultural subsidies or getting licence for opening a business.

Central and state governments in developing countries need to aggressively adopt this model to provide greater governance services to their constituencies, and to enhance the participation of citizens in governance processes. Simultaneously, the civil society groups should demand for such models to enable access to governance information which can improve the quality of lives of people. The model can lose its effectiveness in societies, where the free-flow of information is not possible. This can happen in countries where freedom of speech and expression, or political freedom is restricted, or there are tight governmental controls to censor information. The model also loses its effectiveness in situation of optimal ignorance. This happens when citizens are indifferent / not motivated to act upon information available to them, or when governments and decision-makers take wrong decisions, not because of absence of information, but complete disregard of available information.

### **2.5.2 Comparative Analysis Model**

Comparative Analysis Model is one of the least-used but a high potential e-governance model for developing countries. The model can be used to empower people by comparing cases of bad governance with those of good governance and identifying specific aspects of bad governance, the reasons and people behind them, and how the situation can be improved.

The model is based on using immense capacity of ICT and social media tools to explore given information sets with comparable information available in the public or private domain. For instance, if a given amount of money can build 5 primary schools in District 'A' in a country, then why does the same amount of money build only 2 schools in District 'B'? Could this be because of corruption of officials and contractors involved, or siphoning of money for other things? The outcomes are strategic learnings and empowerment, and can lay the basis for possible action, eg: filing of right to information (RTI) to find where the money went.

Essentially, the model continuously assimilates “best practices” in different areas of governance and uses them as benchmark to evaluate other governance practices. It then uses the result to advocate positive changes or to influence 'public' opinion on existing governance practices. The comparison could be made over a time scale to get a snapshot of the past and the present

situation or could be used to compare the effectiveness of an intervention by comparing two similar situations.

The strength of this model lies in the infinite capacity of digital networks to store varied information and retrieve and transmit it instantly across all geographical and hierarchical barriers.

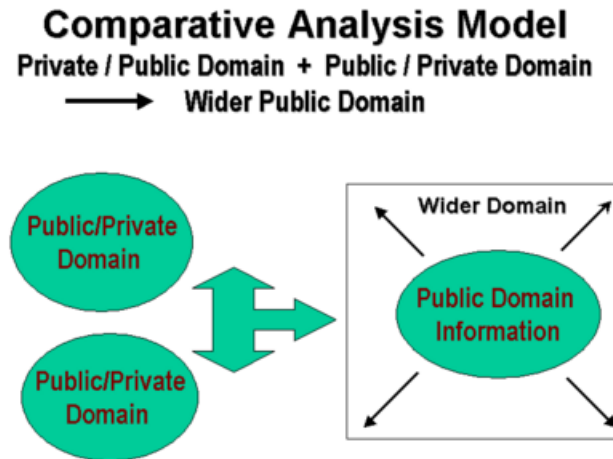


Figure 7: Comparative analysis model

### Application

This model could be applied in the following possible ways:

- To learn from past policies and actions and derive learning lessons for future policy-making.
- To evaluate the effectiveness of the current policies and identify key learnings in terms of strengths and flaws in the policies.
- To effectively establish conditions of Precedence, especially in the case of Judicial or legal decision-making (example for resolving patent-related disputes, public goods ownership rights), and use it to influence/ advocate future decision-making.
- To enable informed decision-making at all levels by enhancing the background knowledge and also providing a rationale for action.
- To evaluate the performance and track-record of a particular decision-maker/ decision-making body.

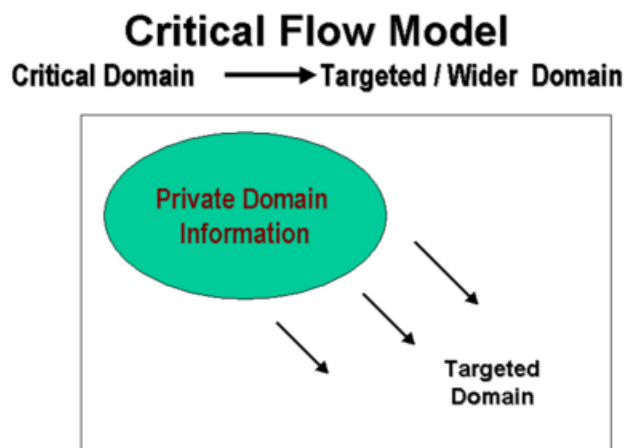
Developing countries could very effectively use this comparative model as ICT opens their access to the global and local knowledge products at a relatively low -cost. The model is very much based on the existing sets of information but requires the ability to analyse and bring out strong arguments which could then be used to catalyze existing efforts towards self governance.

There is a vast scope of application of this model for judicial advocacy as landmark/key judgments of the past could be used as precedence for influencing future decision-making. Further, watch-guard organizations and monitor-groups can use this model to continuously track the governance past record and performance and compare with different information sets. The model however becomes ineffective in absence of a strong civil society interest and public memory which is essential to force decision-makers to improve existing governance practices.

### 2.5.3 Critical Flow Model

The model is based on broadcasting information of 'critical' value (which by its very nature will not be disclosed by those involved with bad governance practices) to targeted audience using ICTs and other tools. Targeted audience may include media, affected parties, opposition parties, judicial bench, independent investigators or the general public.

Those who would divulge such information could include upright officials and workers, whistleblowers, affected parties and those who were themselves involved in bad governance practices but have now changed their minds or may wish to trade such information for lenient punishments.



*Figure 8: Critical flow model*

The use of this model requires a foresight of:

- Understanding the "critical and use value" of a particular information set
- How or from where this information could be obtained
- How could the information be used strategically
- Who are the best target group for such information- the users for whom the availability of this information will make a huge difference

The strength of this model is that the concept of 'distance' and 'time' becomes redundant when information is hosted on a digital network. Once available on the digital network, the information could be used advantageously- by instantly transferring the critical information to its user group located anywhere or by making it freely available in the wider public domain.

## Applications

This model could be applied in the following possible ways:

- Making available corruption related data about a particular Ministry / Division/ Officials online to its electoral constituency or to the concerned regulatory body.
- Making available Research studies, Enquiry reports, Impact studies commissioned by the Government or Independent commissions to the affected parties.
- Making Human Rights Violations cases violations freely available to Judiciary, NGOs and concerned citizens.
- Making available information that is usually suppressed, for instance, Environmental Information on radioactivity spills, effluents discharge, information on green ratings of the company to concerned community.

This model is more directed and evolved in comparison to the Broadcasting/Wider Dissemination Model. Different organizations can use it differently depending on the aspect of governance they situation they want to address. By focusing on the critical aspect of information and locating its likeable users, the model corrects information failure, raising awareness about the bad governance practices, and acts as a hindrance to bad governance practices.

At the same time, the model exerts indirect pressure on the concerned governance institution / policy-making body to move away from optimal ignorance attitude to reform, and take into cognizance the interest and opinion of the masses in decision- making processes.

The model may not work in cases where the governance mechanism does not allow public debates and opinions, and censors all information of critical nature. This model unlike the Broadcasting/ Wider-Dissemination model would be more effective in situations of Optimal Ignorance of the Government. Optimal ignorance occurs when injudicious decisions are taken not in the absence of availability of enough information but because of disregard of information by the decision-makers.

### 2.5.4 E-Advocacy Model

E-Advocacy / Mobilization and Lobbying Model is one of the most frequently used Digital Governance model and has often come to the aid of the global civil society to impact on global decision-making processes. The model is based on setting-up a planned, directed flow of information to build strong virtual allies to complement actions in the real world. Virtual

communities are formed which share similar values and concerns, and these communities in turn link up with or support real-life groups/ activities for concerted action. The model builds the momentum of real-world processes by adding the opinions and concerns expressed by virtual communities. The strength of this model is in its diversity of the virtual community, and the ideas, expertise and resources accumulated through this virtual form of networking. The model is able to mobilize and leverage human resources and information beyond geographical, institutional and bureaucratic barriers, and use it for concerted action.

### Mobilisation and Lobbying Model Networking Networks for Concerted Action

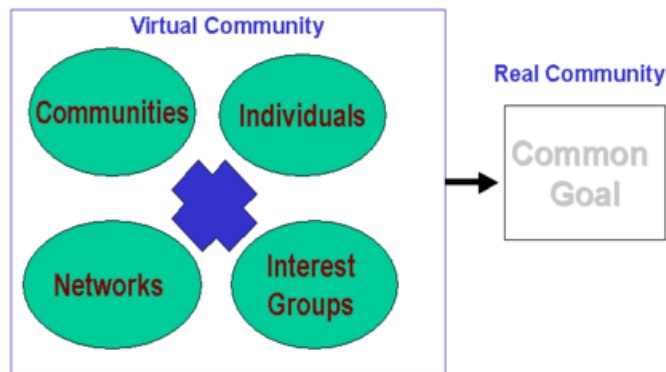


Figure 9: Mobilisation and lobbying model

#### Applications

This model could be applied in the following possible ways:

- Fostering public debates on issue of larger concerns, namely on the themes of upcoming conferences, treaties etc.
- Formation of pressure groups on key issues to force decision-makers to take their concerns into cognisance.
- Making available opinions of a suppressed groups who are not involved in the decision-making process into wider public domain.
- Catalysing wider participation in decision-making processes.
- Building up global expertise on a particular theme in absence of localised information to aid decision-making.

This model has grown manifold since the onset of debates on the Seattle round of World Trade Organisation in 1999, which saw the formation of several virtual communities to express their concerns in the WTO agreements. The display of a unified, informed civil society force at Seattle was in some ways a result of the intensive interaction and exchange of opinion happening over the virtual networks months prior to this WTO summit. There was a lot of concerted actions at the Regional level as an end result of such discussions which built into the global movement.

The model enhances the scope of participation of individuals and communities in debates which affect them and help them build a global alliance. A community may no longer find itself isolated but may find an ally for mobilizing effective action through this model. It also creates an effective deterrent for governments and decision-making bodies who are responsive to people's opinion to provide better governance.

The model could also be used favourably by the government in a positive manner to encourage public debates on issues where the opinion and expertise of civil society is of great importance and therefore could become a tool to enhance democratic practises and improve governance practices (especially in Developing Countries).

### 2.5.5 Interactive Service Model

Interactive-Service model is a consolidation of the other digital governance models and opens up possibilities for one-to-one and self-serviced participation of individuals in governance processes. ICTs have the potential to bring every individual into a digital network and enable interactive (two-ways or multiple-ways) flow of information among them. This potential of ICTs is fully leveraged in this model. As the participation is direct and not through representatives, it can bring greater objectivity and transparency in decision-making processes, and give a greater feeling of involvement and empowerment, provided that individuals are willing to engage in the governance processes.

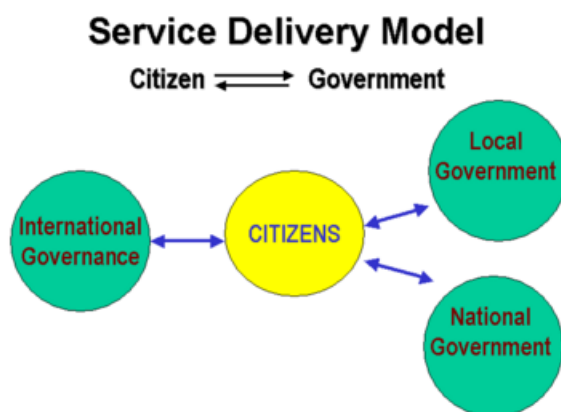


Figure 10: Interactive service model

Under this model, the various services offered by the Government become directly available to its citizens in an interactive manner. It does so by opening up an interactive Government to Consumer to Government (G2C2G) channel in various aspects of governance, such as election of government officials (e-ballots); decision to make on specific issues (eg: health plans), delivery of individualised government services, gauging public mood and opinions, targeting specific communities for specific governance advice or services, bringing mass awareness.

#### Applications

This model could be applied in the following possible ways:

- To establish an interactive communication channels with key policy-makers and members of planning commissions.
- To conduct electronic ballots for the election of government officials and other office bearers.
- To conduct public debates / opinion polls on issues of wider concern before formulation of policies and legislative frameworks.
- Filing of grievances, feedback and reports by citizens with the concerned governmental body.
- Establishing decentralize forms of governance.
- Performing governance functions online such as revenue collection, filing of taxes, governmental procurement, payment transfer etc.

The model firmly relies on the interactive applications of ICT and therefore is a technology and cost - intensive model which will require a transition period before being adopted on a wider scale, especially in the developing countries. It would also require elemental familiarity of ICT among the citizens to fully benefit from this model. Nevertheless, the diminishing costs of ICT and the advantages offered by this technology would certainly catalyze the penetration of this model. Intermediary organisations, knowledge networkers and middlemen will play a tremendous role to play in widespread replication of this model.

## ***2.6 LEGAL AND POLICY FRAMEWORK FOR FACILITATING ICT IN E-GOVERNANCE<sup>16</sup>***

1. **Information Technology Act 2000** - The objective of this Act is "to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic methods of communication commonly referred as "electronic means of communication and storage of information" to facilitate electronic filing of documents with the govt. agencies, and further to amend the IPC, Indian Evidence Act 1872 and the Banker's book Evidence Act 1891 and the Reserve Bank of India Act 1934 and for matters connected therewith or incidental thereto." E-Governance and E-Commerce transactions are covered under the ambit of this Act which facilitates acceptance of electronic records and digital signature. It provides legal framework so that legal sanctity is accorded to all electronic records and other activities carried out by electronic means.
2. **Report Of The Working Group On Convergence And E-Governance 20012-07** - This working group report proposed the need for administration to transform itself from passive information and service provider to a platform for the active involvement of citizens. However, the main drawback of this report was it focused only on public investments and did not visualize the extent of private initiative in the convergence area or in e-commerce and other allied segments. It advocated the need to set up a central body for taking stock of the total IT picture in the country called 'Council for E-

---

<sup>16</sup> <http://www.publicadministrationtheone.blogspot.in/2014/02/e-governance-concept-significance.html>

Governance' or ad hoc 'Commission on re-engineering Administrative procedures for E-Governance'. Or a National Institute of Smart Governance could be set up.

3. **Common Minimum Programme** - The CMP inter-alia states that e-governance will be promoted on a massive scale and solemnly pledged to the country's people that the UPA govt. would be a corruption free, transparent and accountable government and its administration would be a one that is responsible and responsive at all times.
4. **National E-Governance Plan** - The National E-Governance Plan which forms the core infrastructure for effective service delivery has as its elements - Data centres, State wide Area Networks and Common Service Centres to bring about transparency and citizen centric approach in administration.
5. **Expert Committee** - This expert committee had been constituted for amendments in the IT Act 2000 to include the technological developments post IT Act 2000 which submitted its report in Aug 2005. Its recommendations have been displayed on the department of IT to invite public view and suggestions. The expert committee took into consideration and analyzed relevant experiences and international best practices to recommend in its report. The twin objectives of using IT as a tool for socio-economic development and employment generation; and further consolidation of India's position as a major global player in the IT sector.
6. **Right To Information Act 2005** - The Right To Information Act 2005 confers on the citizens the right to:
  - a. Inspect works, documents and records of the govt. and its agencies.
  - b. Take notes, extracts or certified copies of documents or records.
  - c. Take certified samples of material.
  - d. Obtain information in form of print outs, diskettes, floppies, tapes, video cassettes or in any other electronic mode.

This Act has facilitated a two way dialogue between the people and the govt. ensuring transparent and accountable governance to the people in order to make well informed decisions and tackle corruption as well as monitor the functioning of the government.

## ***2.7 SIGNIFICANCE OF E-GOVERNANCE***

ICT applications have the following significance in the process of E-Governance:

- a. **Administrative Development:** ICTs help in reforming administrative processes to a great extent. ICTs help in the following manners:
  - i. *Automation of Administrative Processes* - When there is minimal human intervention and everything is system driven then this leads to effective and efficient as well as timely services. Now departments are computerised and connected through network and software has been built and designed around government depts. ensuring efficiency in operations.
  - ii. *The departments* have launched their own individual websites carrying information of their respective departments enabling online carrying of operations



and file movements as well as budgeting, accounting, data flow, etc. have become easy.

- iii. *Paper-Work Reduction*- Paperwork is reduced to a great extent with communication being enabled via electronic route and storage and retrieval of information in the electronic form. In this concept files and mails (information) are transmitted over wires to small computers at each employees desk and everything is computer managed. SO there is reduction of physical movements and consumption as well as storage of huge piles of paper.
- iv. *Quality Of Services* - ICT facilitates Govt. to deliver services to the citizens with greater accountability, responsiveness and sensitivity since now people are able to get services efficiently and instantaneously as well as economically.
- v. *Online redressal* of grievances ensures officials accountability and also sensitises them. Video tele-conferencing monitoring has further facilitated central supervision, reporting and face to face communication leading to better quality of services.
- vi. *Elimination Of Hierarchy* - Through the introduction of Intranet and LAN there has been a reduction in procedural delays caused by hierarchical processed in organisations as it has become possible to send and receive information and data across various levels in an organisation instantaneously helping the involvement of all levels in decision making.
- vii. *Change in Administrative Culture* - With E-Governance public action has come under public glare thus inducing norms and values of accountability, openness, integrity, fairness, equity, responsibility and justice in the administrative culture freeing it from 'bureau-pathology' and becoming efficient and responsive.

b. **Effective Service Delivery:** The above mentioned has become possible since ICTs ensure -

- i. *Transparency* - Via dissemination and publication of information on the web which involves detailed public scrutiny making the service delivery efficient and accountable.
- ii. *Economic Development* - ICTs reduce transaction costs making services cheaper. To state an example - rural areas suffer on account of lack of information regarding markets, products, agriculture, health, education, weather, etc. and when all of this could be accessed online by them it would evidently lead to better and more opportunities and prosperity in such areas.
- iii. *Social Development* - Access to information empowers citizens as they can participate and voice their concerns which could be accommodated in programme/project formulation, implementation, monitoring and service delivery.

Also, web enabled participation will counter the discriminatory factors affecting our societal behavior.

- iv. *Strategic Information System* - The competitiveness in the organizational sphere today has forced public functionaries to perform to their best ability and this is achieved only when information regarding all aspects are made available to the management at every point in order to make routine as well as strategic decisions which are done effectively via the use of ICTs.

## ***2.8 CHALLENGES IN THE IMPLEMENTATION OF E-GOVERNANCE***

In order to harness the benefits of ICT maximally, there is a need to develop sufficient and adequate infrastructure, provide sufficient capital and investments, enable easy and wider accessibility and generate ample, skillful HR. Let us discuss these challenges in detail.

- i. **Infrastructure** - TO strengthen the infrastructure ' The National Task Force on Information Technology and Software Development' in 1998 recommended broadband connection (also known as 'the last mile') linkage for IT application Service Providers (ASPs),Internet Services Providers(ISPs) and IT promotional organisations either by fiber optics or by radio communication with the aim to ' boost efficiency and enhance market integration' through Internet/Intranet for sustainable regional development.
- ii. **Capital** - High rate of investment in IT capital and supportive environment is necessary to achieve a digital economy. The economy is crunched on resources so the need is to generate resources from the market and private sector. PPP is a step in the right direction to achieve this.
- iii. **Access** - Even though there are more than 10 million users of the Internet in the country, more than 75% of these users are in urban India alone which exposes the reach of the rural and disadvantaged sections. However, Gram Panchayats are being roped in to expand ICTs reach. The National Informatics Centre (NIC) has developed a comprehensive web-based software for Panchayati Raj and rural applications viz. Andhra Pradesh which is a step in the right direction.
- iv. **Utility Of Information** - Information which is of use should be provided in an interesting and appealing manner. A vision document has been prepared for E-Governance by the Government of India and the State Governments. Though Citizen's Charters of many departments are available on the net,further publicity of such facilities is required to enable the public to access the necessary information.
- v. **Human Resources Development** - There exists a dearth of quality manpower in India inspite of growing rate of employment in various sectors. A gap exists between demand and supply in the IT Manpower market. To bridge this gap we need to have more technical institutes to impart quality education and training to build a pool of human resources in the field.

- vi. **Capacity Building** - One needs to be trained in computer skills for effective service delivery. Though this training is being carried out to all the basic public functionaries, yet its effective use of ICT is yet to be seen. Also, there is a need to immediately launch a nationwide 'Train The Teachers' Programme (3T Programme) at all levels including schools and colleges viz. combination of physical and virtual training.
- vii. **Changing the Mindset Of Government Functionaries** - Govt. functionaries need to be reminded and made aware that they are there to serve the people as per the policies and programmes and in order to do that efficiently technological advancement is a facilitator which solves the problems faced by the people. ICT is not a solution in itself. In order to change this mindset of public functionaries there is a need to impart orientation and training programmes to them emphasizing this.
- viii. **Language** - Given the Indian social conditions, unless we develop interface in vernacular languages, it would remain out of reach of many people who are not versed in English. It may be mentioned here that this hurdle is being worked upon and organisations like CDAC has developed multilingual software for this purpose.
- ix. **Standardisation in Data Encoding** - Multiple access points maintained in various languages at various levels need to be updated in conformity with similar standards for data-encoding and application logic for a common horizontal application and data dictionary. This is also important for finding aggregates in the national context.
- x. **Grievance Redressal Mechanism** - Grievance redressal for various functions need to be made necessarily. For this Interactive platforms on the internet may speed up the process and be useful for this purpose.
- xi. A good example of this is the BMC-Praja Foundation's joint initiative of the Online Complaint Management System (OCMS) which is perhaps the world's first citizen-govt. partnership for resolving public grievances in municipal services. It has been in operation since April 2003 and efficiently uses IT as a tool for achieving its results.
- xii. The Central Vigilance Commission has also provided such a platform for people to register their complaints against corrupt officials.  
However, such sporadic instances need to be made more broad-based and effective and more public service agencies need to get into providing such facilities.
- xiii. **Cyber Laws** - Appropriate laws need to be enacted by the govt. which are especially necessary to enable transactions over the Internet. Safety concerns regarding the use of credit cards or other modes of payment inhibits consumers from utilizing online facilities. MTNL Delhi as an example has provided the online facility for payment of telephone bills but not even one percent of its consumers avail it. Therefore, strict and robust cyber laws need to be enacted and efficiently implemented so that confidence is generated in the minds of consumers towards this system to provide online security.

## **2.9 EVOLUTION IN E-GOVERNANCE AND MATURITY MODELS**

### **2.9.1 Difference between E-Government and E-Governance**

Both terms are treated to be the same, however, there is some difference between the two. "E-government" is the use of the ICTs in public administration - combined with organizational change and new skills - to improve public services and democratic processes and to strengthen support to public<sup>17</sup>. The problem in this definition to be congruence definition of e-governance is that there is no provision for governance of ICTs. As a matter of fact, the governance of ICTs requires most probably a substantial increase in regulation and policy-making capabilities, with all the expertise and opinion-shaping processes along the various social stakeholders of these concerns. So, the perspective of the e-governance is "the use of the technologies that both help governing and have to be governed". The Public-Private Partnership (PPP) based e-governance projects are hugely successful in India. United Telecoms Limited known as UTL is a major player in India on PPP based e-governance projects . Each project had mammoth statewide area networks in these states.

Many countries are looking forward to a corruption-free government. E-government is one-way communication protocol whereas e-governance is two-way communication protocol. The essence of e-governance is to reach the beneficiary and ensure that the services intended to reach the desired individual has been met with. There should be an auto-response to support the essence of e-governance, whereby the Government realizes the efficacy of its governance. E-governance is by the governed, for the governed and of the governed.

Establishing the identity of the end beneficiary is a challenge in all citizen-centric services. Statistical information published by governments and world bodies does not always reveal the facts. The best form of e-governance cuts down on unwanted interference of too many layers while delivering governmental services. It depends on good infrastructural setup with the support of local processes and parameters for governments to reach their citizens or end beneficiaries. Budget for planning, development and growth can be derived from well laid out e-governance systems

Maturity models are models of organizational improvement that are built on the observation that organisations involved in complex endeavors move through levels of effectiveness<sup>18</sup>. As organisations become more experienced in those endeavors and develop effective systems supporting the activities, they become more "mature" in their approach. A maturity model is a method for judging the maturity of the processes of an organization and for identifying the key practices that are required to increase the maturity of these processes.

However, in its simplest form, a maturity model is an enumeration of attributes for a sequence of maturity levels<sup>19</sup>. An eGovernment maturity model provides us with guidance on how to gain control of our processes for developing and maintaining eGovernment services and how to

---

<sup>17</sup> <https://en.wikipedia.org/wiki/E-governance>

<sup>18</sup> [http://www.cad.vuw.ac.nz/research/emm/two\\_faq.php](http://www.cad.vuw.ac.nz/research/emm/two_faq.php)

<sup>19</sup> <http://www.windley.com/docs/eGovernment%20Maturity.pdf>

evolve toward a culture of excellence in providing and managing eGovernment(Windley P. J., 2002).

Table 3: e-government maturity model

	Level 1: Simple Website	Level 2: Online Government	Level 3: Integrated Government	Level 4: Transformed Government
<b>Attributes</b>	Static pages Lists of departments and contact information Links to separate departments Policy statements Downloadable forms and documents Access primarily via telephone No site reporting, tracking or analysis	Departmental focus Online forms for applications and registrations Online payment Request information or service via email Respond to online surveys Limited online help, FAQs, resolution services Basic account inquiry Basic benefits enrollment	End-to-end electronic transactions Automated RFP and procurement process Cross-departmental sharing of information Automated advice and problem resolution data Limited configuration capabilities Self-service HR administration Web-based training	Community-centric, integrated, intergovernmental processes Common platform for targeting content through any channel/touch point Internal/external business process integration and collaboration (planning, workflow, design) Constituent case tracking to ensure resolution and satisfaction Highly configurable HR (benefits, career planning, development training)

## 2.9.2 Levels of E-Governance

There are four levels in e-governance<sup>20</sup>:

- a. **Level 1: Information** : In the first phase e-governance means being present on the web, providing the external public with relevant information. The format of the first government websites is similar to that of a brochure or leaflet. The value to the public is that government information is publicly accessible; processes are described and thus become more transparent, which improves democracy and service. Internally (G2G) the government can also disseminate information with static electronic means, such as the Internet. In this phase it is all about information from a single page presence on the web to a website with all relevant government information available to the public. Most governments are at this stage in India, and therefore what they believe is the end of the process is only the beginning.
- b. **Level 2: Interaction**: In the second phase the interaction between government and the public is stimulated with various applications. People can ask questions via e-mail, use search engines for information and are able to download all sorts of forms and documents. These functionalities save time. In fact the complete intake of applications can be done online at all times of the day on all days of the year, instead of only being possible at a physical counter during working hours. Internally government organizations use local networks, intranets and e-mail to communicate and exchange data. The bottom line is that more efficiency and effectiveness is achieved because a large part of the intake is done online. However, you still have to go to the office to finalise the

<sup>20</sup> <http://productivity.tn.nic.in/knowledgebase/egov/Levels%20of%20e-Governance.pdf>

transaction, by paying a fee, handing over evidence or signing papers. A few progressive governments in India started projects in some areas which allow this level of service to occur.

- c. **Level 3: Transaction:** With phase three the complexity of the technology is increasing, but customer value will also be higher. Most complete transactions can be done without going to a government office. Examples of online services are filing income tax, filing property tax, extending/renewal of licenses, visa and passports and online voting. Phase three is mainly complex because of security and personalization issues – e.g. digital signatures are necessary to enable legal transfer of services. On the business side the government is starting with e-procurement applications. In this phase, internal processes have to be redesigned to provide good service. Now the complete process is online, including payments and certification. Only one or two governments in India are at the stage where they are providing this level of service across some functions in a department. And probably there is none that is doing it for all functions in any one department.
- d. **Level 4: Transformation:** The fourth phase if the transformation phase in which all information system are integrated and the public can get all services at one (virtual) counter. One single point of contact for all services is the ultimate goal. The complex aspect in reaching this goal is mainly on the internal side, e.g. the necessity to drastically change culture, processes and responsibilities within the government institution. Government employees in different departments have to work together in a smooth and seamless way. In this phase cost savings, efficiency and customer satisfaction are reaching highest possible levels.

### 2.9.2 e-Governance maturity model

E-Governance Maturity Model EMM V.1 (Dhingra & Misra, 2002) proposes some levels of maturity, depending on the effectiveness with which the e-governance efforts have been initiated, implemented or successfully completed.

- The model also provides for identification of key focus areas that need to be concentrated for attaining a specific maturity level.
- The EMM version 1.0 proposes five levels of maturity, depending upon the effectiveness with which the e-governance efforts have been initiated, pursued, utilized and institutionalized.

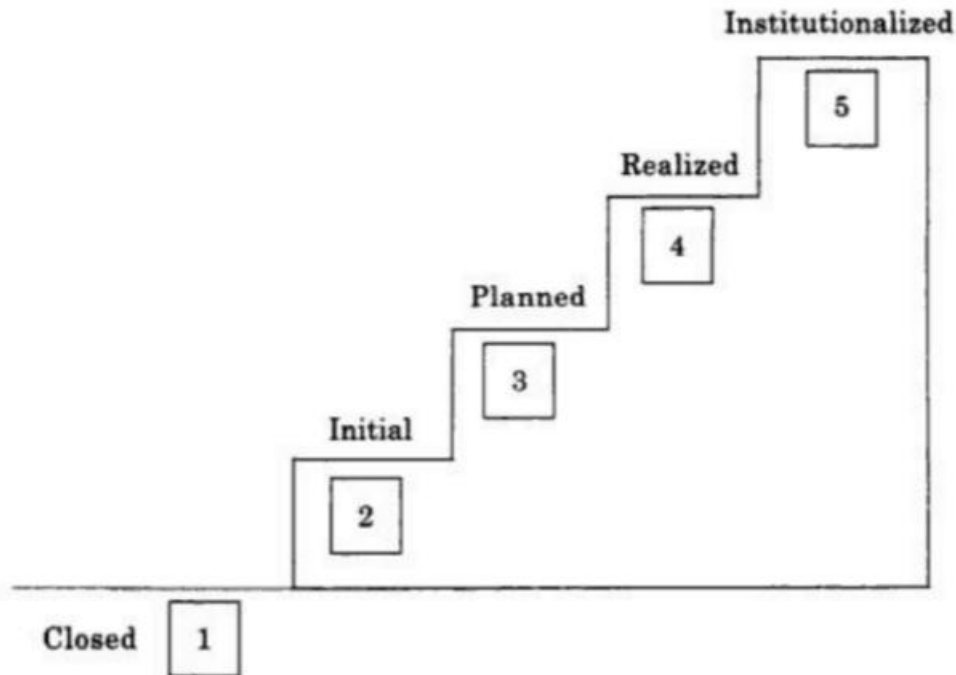


Figure 11: E-Governance maturity levels

#### **LEVEL 1: Closed**<sup>21</sup>

- Here an organization does not use ICT as a facilitator for good governance and has no plans to do so in the near future.
- Such situation may arise due to lack of exposure to ICTs and associated benefits that again may depend upon a number of reasons: remoteness, lack of resources and strategic thinking.
- As a result the organization is closed in terms of being connected and sharing of information in the context of “E-governance”.
- However, even in this condition the organization may be efficiently functioning.

#### **LEVEL 2: Initial**

- This level corresponds to the stage when an organization has initiated the automation of its processes but on a ad-hoc basis.
- No organized efforts are made to undertake the e-governance initiatives.
- Many of such efforts are abandoned due to lack of proper direction

#### **LEVEL 3: Planned**

- This level comprises of systematic approaches with clearly defined vision, objectives and goals for e- governance.
- Need assessments are made to prioritize the areas of implementation and measure the extent of e-readiness.

<sup>21</sup> <http://documents.mx/documents/e-governance-models-unit-2.html>

- Taking necessary input from need assessment study, extensive planning has been carried out indicating policies, strategies, various activities, stakeholders, roles and responsibilities and resources required in terms of time, money and manpower to undertake the e-governance exercise.

**LEVEL 4: Realized**

- This level corresponds to the stage when the organization actually realizes the complete e-governance plan.
- Consequently, an integrated system is established where all the internal processes of the organization are computerized and there is a seamless information exchange among all concerned entities.
- The organization starts delivering the services to its external as well as internal customers in an effective manner.
- Complete realization of the plan, in a single instance, would entail enormous amount of resources in terms of time, money and manpower which may necessitate adopting a phased approach for operationalizing the e-governance services.
- Retrospected: At this level, the organization has retrospectively studied its business processes in view of its vision, overall e-governance objectives, the service-oriented approach and changes, if required, in the processes are initiated as a constant evolutionary process.
- E-ready: In this stage, e-readiness essentials, which are also the building blocks for e-governance, are ensured by the organization.
- Partially open: At this stage some of the e-governance services are operationalized resulting in a partial information exchange among the entities both within and outside the organization.
- Open: This sub-level of realized state implies complete deployment of e-governance services that ensure an integrated system that is open to information exchange. The focus here shifts from acquiring and implementing “e” enabling factors to effectiveness to deal with the customer needs and is accountable for its services.

**LEVEL 5: Institutionalized**

- At this level, the organization sustains the realized state over a period of time so that e-governance becomes part of its work culture. The e-governance services are effectively utilized and accepted by the users. Several iterations between planned and realized state lead to institutionalization, when e-governance becomes a way of life.
- E-Readiness Essentials
  - presence of strategic thinking, leadership and commitment among top-level decision makers
  - Institutional Infrastructure
  - ICT Infrastructure
  - Human Capacities
  - Legal Infrastructure



For further details of the above, the readers are advised to refer the following link:

<http://documents.mx/documents/e-governance-models-unit-2.html>

## **2.10 DIGITAL INDIA PROGRAM**

The Digital India programme is a flagship programme of the Government of India with a vision to transform India into a digitally empowered society and knowledge economy<sup>22</sup>. The journey of e-Governance initiatives in India took a broader dimension in mid 90s for wider sectoral applications with emphasis on citizen-centric services. Later on, many States/UTs started various e-Governance projects. Though these e-Governance projects were citizen-centric, they could make lesser than the desired impact. Government of India launched National e-Governance Plan (NeGP) in 2006. 31 Mission Mode Projects covering various domains were initiated. Despite the successful implementation of many e-Governance projects across the country, e-Governance as a whole has not been able to make the desired impact and fulfill all its objectives.

It has been felt that a lot more thrust is required to ensure e-Governance in the country promote inclusive growth that covers electronic services, products, devices and job opportunities. Moreover, electronic manufacturing in the country needs to be strengthened.

In order to transform the entire ecosystem of public services through the use of information technology, the Government of India has launched the Digital India programme with the vision to transform India into a digitally empowered society and knowledge economy.

Digital India has three core components<sup>23</sup>. These include:

- The creation of digital infrastructure
- Delivering services digitally
- Digital literacy

There are nine pillars of Digital India Programme.

1. Broadband Highways
2. Universal Access to Mobile Connectivity
3. Public Internet Access Programme
4. e-Governance – Reforming Government through Technology
5. eKranti - Electronic delivery of services
6. Information for All
7. Electronics Manufacturing
8. IT for Jobs
9. Early Harvest Programmes

### **2.10.1 Services**

Some of the facilities which will be provided through this initiative are Digital Locker, e-education, e-health, e-sign and national scholarship portal. As the part of Digital India, Indian government planned to launch Botnet cleaning centers.

---

<sup>22</sup> <http://www.digitalindia.gov.in/content/about-programme>

<sup>23</sup> [https://en.wikipedia.org/wiki/Digital\\_India](https://en.wikipedia.org/wiki/Digital_India)

1. **DigiLocker:** Digital Locker facility will help citizens to digitally store their important documents like PAN card, passport, mark sheets and degree certificates. Digital Locker will provide secure access to Government issued documents. It uses authenticity services provided by Aadhaar. It is aimed at eliminating the use of physical documents and enables sharing of verified electronic documents across government agencies.
2. **Attendance.gov.in:** Attendance.gov.in is a website, launched by PM Narendra Modi on 1 July 2015 to keep a record of the attendance of Government employees on a real-time basis. This initiative started with implementation of a common Biometric Attendance System (BAS) in the central government offices located in Delhi.
3. **MyGov.in:** MyGov.in is a platform to share inputs and ideas on matters of policy and governance.

## ***2.11 TOWARDS GOOD GOVERNANCE THROUGH E-GOVERNANCE MODELS***

The changes brought about in the citizen-government relationship through digital governance are fourfold:

- They open up avenues for flow of information both vertically and laterally, and thus encompass a wider foundation of the civil society. A greater density of information flow is achieved – between government and civil society, amidst the government or within the civil society itself. The right to voice and expression therefore gets more frequently exercised by citizens who wish to engage in the political processes.
- Information becomes difficult to be capitalized by a few for political gains and at the expense of ignorance of citizens. Digital governance ensures that the power-equations shift from being concentrated and restricted at selected nodes to its more even and timely distribution among citizens, opposition parties and watch guard groups.
- There is a greater scope to influence policy-makers and members of the civil society through collective opinion casting, direct participation, participation in public debates, and use of advocacy tools.
- Policy-makers become more aware of the voices of people and can effectively involve them in policy-making mechanisms. They realize that their actions are under the scrutiny of many more watch guard organizations and there are greater avenues available with people to obtain or triangulate information from different sources. Information also becomes difficult to obliterate and is forever archived to increase the institutional memory of the society.

## ***2.12 SUMMARY***

1. Through e-governance, government services are made available to citizens in a convenient, efficient and transparent manner.
2. E-Governance is about reform in governance, facilitated by the creative use of Information and Communications Technology.

3. The aim of e-governance is bringing in faster and transparent service delivery, accountability, information sharing and people participation in the decision making and govt. processes.
4. Recognising the increasing importance of electronics, the Government of India established the Department of Electronics in 1970
5. Rapid growth of communications technology and its adoption in governance would help in bringing government machinery to the doorsteps of the citizens.
6. Digital Governance models keep on expanding and evolving as new applications of ICTs come to light and to deal with new issues in the area of governance.
7. The National E-Governance Plan which forms the core infrastructure for effective service delivery has as its elements - Data centres, State wide Area Networks and Common Service Centres to bring about transparency and citizen centric approach in administration.

### ***2.13 CHECK YOUR PROGRESS***

- [1].\_\_\_\_\_ would make available timely and reliable information on various aspects of governance.
- [2].The complete transformation of the processes of Governance using the implementation of Information & Communication Technology is called\_\_\_\_\_.
- [3].\_\_\_\_\_ model is based on mass dissemination of governance-related information which is already available in the public domain into the wider public domain using ICTs.
- [4].Comparative Analysis Model is one of the least-used but a high potential e-governance model for \_\_\_\_\_ countries.
- [5].\_\_\_\_\_ model is also known as Mobilization and Lobbying Model.
- [6].E-Governance and \_\_\_\_\_ transactions are covered under the ambit of Information Technology Act 2000 which facilitates acceptance of electronic records and digital signature.
- [7].\_\_\_\_\_ are models of organizational improvement that are built on the observation that organisations involved in complex endeavors move through levels of effectiveness

### ***2.14 ANSWERS TO CHECK YOUR PROGRESS***

- [1].ICT
- [2].E-Governance
- [3].Broadcasting
- [4].Developing
- [5].E-Advocacy
- [6].E-Commerce
- [7].Maturity models

### ***2.15 MODEL QUESTIONS***

1. What is e –governance? What are the goals of e-governance?

2. What are the benefits of e-governance?
3. What are the basic models of e-governance? Explain each model in details.
4. Explain legal and policy framework for facilitating ICT in e-governance.
5. What is the significance of e-governance?
6. What are the challenges in the implementation of e-governance?
7. What is the difference between e-government and e-governance?
8. Explain the different levels of e-governance.
9. Discuss digital India program.

## UNIT III: E-READINESS

### 3.1 LEARNING OBJECTIVES

After going through this unit, you will be able to:

- Understand the stages in e-governance.
- Know the benefits of e-governance.
- Understand e-readiness issues in the implementation of e-governance.

### 3.2 STAGES IN E-GOVERNANCE

Many governments initiate projects haphazardly, without any careful planning that takes into account what stage must precede another for the succeeding one to be successful<sup>24</sup>. Common sense reveals that there are 4 general stages, which in most cases, must follow each other.

**A. Stage 1: Information Technology Frameworks:** Deployment of a basic Information Technology framework is a prerequisite for any foray into e-Governance. By basic we mean:

- a. Computers in some minimum number and with some minimum capability
- b. Interconnectivity of those computers (networking)
- c. Basic bandwidth for applications like internet access and email
- d. A communication platform – such as an intranet

The development of an Intranet – an internal ‘internet’ – for the employees and constituents of the Government agency – for centralized access to collaborative work tools and information will dramatically increase efficiency by creating a tap on common knowledge pool as well as providing productivity tools. The choice of computers is relatively easy, however, the software is more critical a component than the hardware. The price of a PC is pushed up by the cost of license for commercial software. Open Source software which is available without fee for license, can help enormous amounts of money as well as save government from a very dangerous strategic error.

**B. Stage 2: Digitisation:** Once technology has been deployed and a network put in place, the next step is to make sure that all content and processes of the administration is digitized. Processes and systems should ensure that digitization and tagging of documents becomes a habit, not one isolated project. Digitisation and tagging ensures that time is saved in mundane tasks like locating files. If the digitization process does not take place, the purpose of implementing e-governance is defeated. How can you talk about providing better services to the citizens unless the department is internally equipped to provide those services?

**C. Stage 3: Citizens Access:** Once the digitization process has become a process, the next logical step for an administration is to make the information available to the citizens. One way of doing this is through a ‘Citizens Portal’ essentially involve transforming the information produced by the Government to make it interactive, attractive and user –

<sup>24</sup> <http://productivity.tn.nic.in/knowledgebase/egov/Stages%20of%20e-Governance.pdf>

friendly, and then allowing it to be accessed by citizens. This can change the experience that citizens have with the administration and also increases the productivity of the officers by saving their time from routine requirements of the general public.

- D. Stage 4: Content:** Even though Governments are one of the richest source of information, the content generated by the government fails to involve the citizen. This is very dangerous because ultimately, after all the computers and networks and state wide fibre optic connections are ready, the thing that will ensure the success or failure of e-governance is the content that flows through those networks. Managing this last link to the citizen is a challenge and unfortunately, has been one in which Government around the world have been singularly unsuccessful in.

### ***3.3 E-READINESS***

There will be problems and challenges, the point however is to prepare to combat them. On a practical level, it is not always the hidden political agenda or lack of resources or the problem of culture that sabotages e-Governance initiatives. Very often, lack of readiness contributes most to the failure. Six key questions can be asked of any government agency in order to assess how strategically prepared they are for e-governance.

#### **3.3.1 Is the Technology Infrastructure Ready?**

Are the computer systems, management system, records and work processes in place to provide the quantity and quality of data to support the move to e-governance? In many departments, data quality is very poor, and there are few mechanisms to address these issues.

#### **3.3.2 Is the Legal Infrastructure Ready?**

Are the laws and regulations required to permit and to support the move to e-governance in place? In many countries, for example, digital signatures cannot be accepted. Or in many departments, due to the lack of a Right to information Act, there is great resistance to allowing transparency.

#### **3.3.3 Is the Institutional Infrastructure Ready?**

E-Governance can only be progressed if the institutions exist to act as a focus for awareness and to act as a means for facilitation of e-Governance. In many countries, there are no institutions to coordinate and lead and drive e-governance.

#### **3.3.4 Is the Human Infrastructure Ready?**

Are the attitudes, knowledge and skills in place that is required to initiate, implement and sustain e-governance initiatives? In many departments, key skillgaps can make the entire exercise pointless even before it starts. There are also 'mindset' gaps – resistance to change, lack of customer-orientation; resistance to information sharing.

#### **3.3.5 Is the Technology framework Ready?**

If all you have is a set of PC's without the underlying technologies to leverage them, then the project is a non-starter. Basic are e-mail, internet access and some form of intranet-based groupware applications no matter how simple or primitive it may be.

### 3.3.6 Is the Leadership and Strategic Thinking Ready?

A critical pre-condition in successful e-Governance is a champion or a small group of champions; leaders with vision who put e-Governance onto the agenda and make it happen. Many cases show that such leadership can smash through many operational barriers. Conversely, all the operational readiness in the world is of limited value if there is no vision and leadership to give direction.

## 3.4 BENEFITS OF E-GOVERNANCE

There are thousands of ways in which intelligent bureaucrats and politicians around the world are using e-governance initiatives to bring about a positive change in the government citizen interaction. Here are a few examples:

- a. **Simpler Documentation- Digitisation of Land Records:** One of the major problems a member of the public face is to get access to their land records. In many countries, this has been one of the priority areas for application of IT. Coupled with GIS, the decentralized databases can hold the local level land records allowing easy access through dedicated terminals. The transfer and registration of deeds can also be made much easier. The implementation of a nation-wide project would eliminate a lot of hassle for all citizens and can bring the fruits of IT revolution to the doorsteps of ordinary citizens. This will also drastically reduce the number of litigations arising from land-related disputes.
- b. **Faster Applications- Redressing Public Grievances:** Under the present system, citizens can ventilate their governance through applications/letters addressed to appropriate authorities. Unfortunately, acknowledgement of receipt of these letters and responding to these letters are almost totally absent in our “government culture”. In the absence of such mechanism, many of the citizens have to spend a lot of efforts to get access to Minister or other high officials. Our Constitution provides for the creation of an office of Ombudsman but even through almost three decades have elapsed since adoption of the Constitution; we are yet to see its implementation. Many countries have introduced the system of using e-mails to ventilate the grievances with a lot of success. In fact, homepages of the Head of Government and Ministers in many countries contain a link for directly sending e-mails to them. These are acknowledged within a few minute (sometimes using Auto responder software) and the actions taken are intimated within a few days.
- c. **Simpler Procurement- Goods and Services at lower cost:** The Government in our country is still the largest purchaser of various goods and largest user of services (such as consultancy services) and implementation agency for various construction projects. The rules require competitive bidding for all but the smallest of purchases (which can be done through spot quotations). In order to meet the procedural requirements, advertisement in newspaper is mandatory. With the proliferation of newspapers in the country, it is very difficult for intending suppliers to keep track of all these notices. These problems can be eliminated by resorting to use of internet. For example, the web sites of the agencies can

have all the procurement notices along with the relevant details (e.g. specifications, eligibility criteria, and bidding document) which can be downloaded by the bidders. At a later stage, the responses (like tender or consultancy proposals) can also be submitted using electric communication. This is now recognized as a form of e-Commerce abbreviated as B2G (Business to Government).

- d. Greater Reach of Services- Making the most of limited resources:** One of the major weaknesses in our health care system (particularly in the rural areas) is the lack of availability trained doctors. It may not be possible to post specialist doctors in every village. However, if these centers are connected to district level hospitals and national hospitals that have specialists in various medical disciplines, a doctor or a paramedic can get online advice related to a patient.
- e. Accelerating Education-Doing more with less money:** Information technology can significantly contribute to improvement of our education system in a number of areas, e.g. in managing the large number of educational institutions (particularly the primary and secondary schools) as well as in actual delivery of education. The present school system suffers from a lack of trained teachers, and therefore CD-based courseware or video-based distance education programs can be of great assistance to the teachers as well as students to overcome some of the weaknesses. Moreover, once the schools are connected to the Internet, the students and teachers can have access to most of the well-known libraries in the world, where books, periodicals and reports in digital format are freely available. The development of a Distance Learning System with courses delivered over the Internet can be of great help at all levels of education and training. The results of all public examinations can also be put on the Web.
- f. Public Participation- Making Legislation interactive:** The present system of enactment of legislation does not have much scope for public participation. In fact, in almost all parliamentary debates related to any bill, we see the Members of Parliament from the opposition proposing that the bill be sent for eliciting public opinion but the proposal is almost never accepted. However, the Internet provides an easy route for getting public opinion.
- g. Simplifying Transactions-Payment of Utility Bills:** In urban areas, almost all the households have to interact with various utility agencies like power supply, water supply, gas and telecommunications. Even in the routine this is a tiresome task and very often a user has a grievance of an inaccurate bill which requires a number of visits to various offices for resolution. These can be resolved through electric communication which can be carried out by the consumer at his own convenience rather than wasting valuable office time. The inconvenience of payment of bills can be avoided by resorting to electric fund transfer.
- h. Inexpensive Deterrent- Maintaining Law and Order:** The installation of inexpensive Web cams connected to Police Headquarters for continuous recording at selected locations in large urban areas can be a deterrent to crime, as has been the experience of



some cities in Western Europe. Filing of FIRs over the Internet has also been used with success in some countries. Computers have been successfully used for storage of information about crimes and criminals. By providing access to these databases from different police stations or even hand held devices by police officials on the move, the job of tracking down criminals has become relatively easier.

- i. Inexpensive Deterrent- Post Offices:** All the post offices in many countries have been connected to the internet. This enables the transmission of e-mails by members of public and hand delivery to the recipients (who do not have access to Internet). Moreover, public kiosks can be located in these post offices to enable member of public to send and receive e-mails.
- j. Simplifying Interaction- Municipalities:** Members of the public often have to interact with the City Corporation or Municipality offices for a variety of services like the payment of holding tax, obtaining trade licenses, registration of births and deaths. These interactions can easily be carried out over the Internet.
- k. Incentive for Payment- Making Taxes and Levies easier:** As Electronic Fund Transfer gains popularity, many of the taxes and levies which the citizens have to pay may also be paid through the internet through debit or credit cards. The filing of income tax returns can also be done through the internet.
- l. Making Recruitment Faster- Hiring Personnel:** The government and government agencies are still the largest employers in our country. Thousands of employees are recruited at different levels every year. A central government web site can be developed to provide all the recruitment announcements, so that the applicants need not scan the large number of newspapers, which in many cases are difficult to access from rural areas. The next step would be the electronic submission of applications to the relevant agencies through e-mails. The web sites of these agencies can also provide the information related to latest status of the application.
- m. Making a Permanent Library- Policy Documents for reference:** All policy documents of government can be placed on the Web and be constantly updated. For example, documents like the Budget, specific plans can be placed alongwith the official gazettes. There are limitless possibilities. What must be understood is that once there is a clear understanding of the issues involved and the sincerity to resolve them, there can be an amazing number of innovations in governance.

### **3.5 SUMMARY**

1. Many governments initiate projects haphazardly, without any careful planning that takes into account what stage must precede another for the succeeding one to be successful.
2. There will be problems and challenges, the point however is to prepare to combat them.
3. On a practical level, it is not always the hidden political agenda or lack of resources or the problem of culture that sabotages e-Governance initiatives.

4. There are thousands of ways in which intelligent bureaucrats and politicians around the world are using e-governance initiatives to bring about a positive change in the government citizen interaction.

### ***3.6 MODEL QUESTIONS***

1. What are the different stages of e-governance?
2. What are the benefits of e-governance?
3. How digitization is helpful in the successful implementation of e-governance?
4. Discuss in details the six key questions that can be asked of any government agency in order to assess how strategically prepared they are for e-governance.
5. There are thousands of ways in which intelligent bureaucrats and politicians around the world are using e-governance initiatives to bring about a positive change in the government citizen interaction.

## UNIT IV: E-COMMERCE

### 4.1 LEARNING OBJECTIVES

After going through this unit, you will be able to:

- Know about e-commerce.
- Know the technology infrastructure required for e-commerce.
- Understand various models of e-commerce.
- Understand e-payment.

### 4.2 INTRODUCTION

As the Internet and World Wide Web become commonly use in every household in recent years, it is obvious that e-commerce, a branch of technology and business are incredibly rising<sup>25</sup>. There are more and more E-commerce sites available on the Internet, including the few famous sites such as Amazon, eBay, and Dell. Many major industries have noticed the significant rise of the Internet, so they started selling products through their websites and even have delivery services for customers. Therefore, it is possible to buy everything through the Internet nowadays. You can buy your computer from Dell's website, do your grocery shopping through Loblaws's website, buy your clothes through major clothing industries like Guess or Bluenotes, and even buy your books and electronic products through Future Shop or Best Buy. But industries often perform delivery with extra charge, or simply include the charge on the price listed. E-commerce had become more popular globally, and there are some issues, challenges, and opportunities that need to be identified using the e-commerce sites. There are some aspects for successful globalized e-commerce sites, in which they have multi-lingual support, multi-language customer care, international shipping, and other aspects. Also, this essay would talk about how e-commerce transactions works along with the changes and the benefits that have received by using the e-commerce sites

### 4.3 E-COMMERCE

Electronic commerce, in a broad sense, is the use of computer networks to improve organizational performance. Increasing profitability, gaining market share, improving customer service, and delivering products faster are some of the organizational performance gains possible with electronic commerce<sup>26</sup>. Electronic commerce is more than ordering goods from an on-line catalog. It involves all aspects of an organization's electronic interactions with its stakeholders, the people who determine the future of the organization. Thus, electronic commerce includes activities such as establishing a Web page to support investor relations or communicating electronically with college students who are potential employees. In brief, electronic commerce involves the use of information technology to enhance communications and transactions with all

---

<sup>25</sup> <https://ccit205.wikispaces.com/E-commerce>

<sup>26</sup> <http://opentextbc.ca/electroniccommerce/chapter/introduction/>

of an organization's stakeholders. Such stakeholders include customers, suppliers, government regulators, financial institutions, managers, employees, and the public at large.

According to Beekman, "Electronic Commerce, or e-commerce, is the process of sharing business information, maintaining business relationships and conducting business transactions through the use of telecommunications networks."<sup>27</sup>

### 4.3.1 Advantages of E-Commerce

Many people doubt e-commerce benefits from developing countries. In fact, there are several advantages. Firstly e-commerce lowers the cost for people who wish to become an online merchant. A modest investment in personal computer and internet connection cost can start a business online. Through the World Wide Web, you can access e-commerce sites from different countries. For a global e-commerce site, there are concerns about language barrier, tariff of the country on shipments, currency rate, and other many concerns. Dell computer corp. is a good example of a successful global e-commerce business. David Dix, the Global Internet PR manager says that when Dell computers went global, they tripled its sales on the Internet to 18 millions every single day. There are some aspects of the global e-commerce sites, in which they have to convert their sites to fit local languages, provide multi-language customer service, convert their sites to fit culturally relevant content, and provide currency checkers for selling products oversea. As e-commerce is accessible on a global scale, it can surely attract more international customers to the site. The IDC report pointed out that there are about 57 million web users just in Japan alone. According to Forrester, Japan could possibly produce a revenue of \$1.6 trillion for the online shopping. Think about how many people are in the world? The global nature of e-commerce can definitely create a new economy.

Some of the advantages of e-commerce are:

- E-commerce also makes findings a lot quicker and easier as say the shop is far away from your house you can check if the product is available before you go and see it. Access and availability are two main benefits.
- For suppliers, it's easier to source products from a wider base and as mentioned, for a cheaper cost
- Saves cost in other administrative processes such as invoices can be sent online saving mass amounts of paper
- it makes your business seem bigger than you really are because your market increases
- the ability to reply to customers and answer queries quicker and cheaper via email definitely helps in sustaining the market and its customers

### 4.3.2 Challenges in E-Commerce

Although e-commerce is quite convenient, there are some issues that keep consumers away from online shopping. Online fraud will be the most common issue for e-commerce. From conducted researches, it was found that online credit card scams are 12 times higher than if a consumer purchase the product in the store. As a result, consumers lack the confidence to shop online.

---

<sup>27</sup> <https://itgs.wikispaces.com/E-Commerce>

Harris Interactive says that approximate 70 percent of consumers worry about the transaction being insecure online, and this lead to a \$15 billion drop in online purchasing. Online commerce sites should be really careful about the security of the transactions. Protect online privacy is a big challenge for the commerce site. When you purchase on the Internet, first thing you need to do is to create an account using your credit card number, address, name, birthday, and basically all your information. Many consumers would fear that their private information would be given out to strangers without any sign, and this would lead to consumers unwilling to give out information on the Internet. The sites should post a privacy statement that clearly states how personal information will be used and whether the information is going to be used beyond the transaction. One of the surveys says consumers will leave the sites if the privacy policy is unclear. A successful website should provide secure transaction for the consumers and protect consumer privacy.

A variety of demographics are resistant to change or prefer to safeguard their personal information. Although it seems hard to find fault in such a marvellous technology, there is a significant market segment that is resistant to accept everything digital, with good reason. Many people are quite hesitant about revealing personal credit information, to a company that exists in a non-physical environment, in exchange for physical goods. For example, internet statistics show that key segments of the population are still either not participating in e-commerce or resistant to join the online community at all. “Globally, almost three-quarters (72 percent) of respondents say they are concerned about online security, especially the potential misuse of their credit cards”. However, many of these fears and misinterpretations are without warrant and are based solely on rumour and media exploitation. “Only 1 percent of adults surveyed say they have been the victim of online fraud and just 6 percent say they know of someone who has been”. Consequently, e-commerce expansion has suffered, thereby limiting its appeal to those who view the security technology trustworthy and reliable. A major challenge to toppling this myth has been assuring users that their most private information will not be used by any third party to target them with malicious or frivolous content.

Some of the disadvantages of E-Commerce are:

- It is hard to ensure that people will visit your site because there are millions of sites out there-more difficult to reach the market directly.
- Most people tend to prefer shopping because they can physically try on everything and know exactly what it looks like or touch or feel the product. the social and voyeuristic aspect of shopping is more popular than E commerce hence one may not profit from E commerce.
- The risk of fraud is always there, as online shopping can be dangerous and hence if people don't trust or are apprehensive of sending out credit card information, etc. they may not shop online for less developed countries access to internet is either nil or slow, so not everyone has equal access to the benefits of E commerce. Those companies may

not be able to publicize or advertise themselves as much as those who have the money and the infrastructure in their residing countries to do so.

#### ***4.4 E-COMMERCE BUSINESS MODELS***

There are multiple types of sales scenario some of it are as follows:

- a. **Business-to-Consumer (B2C):** In a Business-to-Consumer E-commerce environment, companies sell their online goods to consumers who are the end users of their products or services. Usually, B2C E-commerce web shops have an open access for any visitor and user.
- b. **Business-to-Business (B2B):** In a Business-to-Business E-commerce environment, companies sell their online goods to other companies without being engaged in sales to consumers. In most B2B E-commerce environments entering the web shop will require a log in. B2B web shop usually contains customer-specific pricing, customer-specific assortments and customer-specific discounts. There are several SaaS B2B eCommerce platforms available, such as TradeGecko's B2B eCommerce Platform.
- c. **Consumer-to-Business (C2B):** In a Consumer-to-Business E-commerce environment, consumers usually post their products or services online on which companies can post their bids. A consumer reviews the bids and selects the company that meets his price expectations.
- d. **Consumer-to-Consumer (C2C):** In a Consumer-to-Consumer E-commerce environment consumers sell their online goods to other consumers. A well-known example is eBay.

#### ***4.5 INFRASTRUCTURE***

Electronic commerce is built on top of a number of different technologies<sup>28</sup>. These various technologies created a layered, integrated infrastructure that permits the development and deployment of electronic commerce applications.

---

<sup>28</sup> Section 4.4 onwards are thankfully adopted from <http://opentextbc.ca/electroniccommerce/chapter/electronic-commerce-technology/> available under creative commons attribution license.

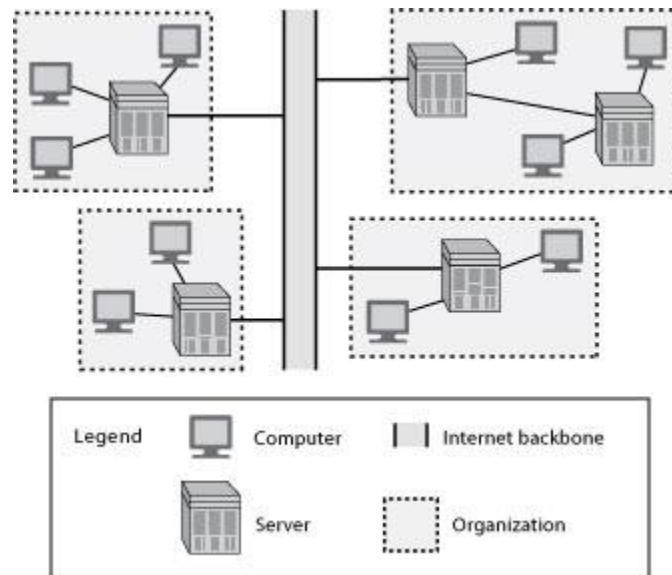


Figure 12: The Internet

Each layer is founded on the layer below it and cannot function without it.

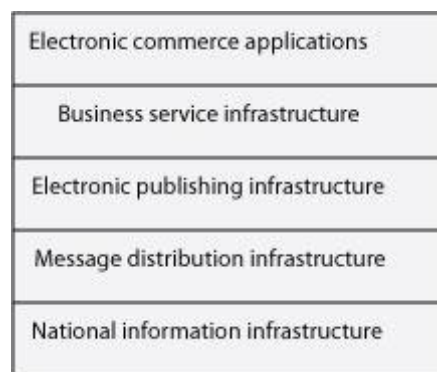


Figure 13: Electronic commerce infrastructure

#### 4.5.1 National Information Infrastructure

This layer is the bedrock of electronic commerce because all traffic must be transmitted by one or more of the communication networks comprising the national information infrastructure (NII). The components of an NII include the TV and radio broadcast industries, cable TV, telephone networks, cellular communication systems, computer networks, and the Internet. The trend in many countries is to increase competition among the various elements of the NII to increase its overall efficiency because it is believed that an NII is critical to the creation of national wealth.

#### 4.5.2 Message Distribution Infrastructure

This layer consists of software for sending and receiving messages. Its purpose is to deliver a message from a server to a client. For example, it could move an HTML file from a Web server to a client running Netscape. Messages can be unformatted (e.g., e-mail) or formatted (e.g., a

purchase order). Electronic data interchange (EDI), e-mail, and hypertext text transfer protocol (HTTP) are examples of messaging software.

### 4.5.3 Electronic Publishing Infrastructure

Concerned with content, the Web is a very good example of this layer. It permits organizations to publish a full range of text and multimedia. There are three key elements of the Web:

- A uniform resource locator (URL), which is used to uniquely identify any server;
- A network protocol;
- A structured markup language, HTML.

Notice that the electronic publishing layer is still concerned with some of the issues solved by TCP/IP for the Internet part of the NII layer. There is still a need to consider addressability (i.e., a URL) and have a common language across the network (i.e., HTTP and HTML). However, these are built upon the previous layer, in the case of a URL, or at a higher level, in the case of HTML.

### 4.5.4 Business Services Infrastructure

The principal purpose of this layer is to support common business processes. Nearly every business is concerned with collecting payment for the goods and services it sells. Thus, the business services layer supports secure transmission of credit card numbers by providing encryption and electronic funds transfer. Furthermore, the business services layer should include facilities for encryption and authentication .

### 4.5.5 Electronic Commerce Application

Finally, on top of all the other layers sits an application. Consider the case of a book seller with an on-line catalog (see Table 4). The application is a book catalog; encryption is used to protect a customer's credit card number; the application is written in HTML; HTTP is the messaging protocol; and the Internet physically transports messages between the book seller and customer.

*Table 4: An electronic commerce application*

Electronic commerce applications	Book catalog
Business services infrastructure	Encryption
Electronic publishing infrastructure	HTML
Message distribution infrastructure	HTTP
National information infrastructure	Internet



## 4.6 PAYMENT SYSTEMS

When commerce goes electronic, the means of paying for goods and services must also go electronic<sup>29</sup>. Paper-based payment systems cannot support the speed, security, privacy, and internationalization necessary for electronic commerce. In this section, we discuss five methods of electronic payment:

- electronic funds transfer
- digital cash
- ecash
- credit card
- Google Wallet

There are four fundamental concerns regarding electronic money: security, authentication, anonymity, and divisibility. Consumers and organizations need to be assured that their on-line orders are protected, and organizations must be able to transfer securely many millions of dollars. Buyers and sellers must be able to verify that the electronic money they receive is real; consumers must have faith in electronic currency. Transactions, when required, should remain confidential. Electronic currency must be spendable in small amounts (e.g., less than one-tenth of a cent) so that high-volume, small-value Internet transactions are feasible (e.g., paying 0.1 cent to read an article in an encyclopedia). The various approaches to electronic money vary in their capability to solve these concerns (see Table 5).

*Table 5: Characteristics of electronic money*

	Security	Authentication	Anonymity	Divisibility
EFT	High	High	Low	Yes
Digital cash	Medium	High	High	Yes
Ecash	High	High	High	Yes
Credit card	High	High	Low	Yes

Any money system, real or electronic, must have a reasonable level of security and a high level of authentication, otherwise people will not use it. All electronic money systems are potentially divisible. There is a need, however, to adapt some systems so that transactions can be automated. For example, you do not want to have to type your full credit card details each time you spend one-tenth of a cent. A modified credit card system, which automatically sends previously stored details from your personal computer, could be used for small transactions.

The technical problems of electronic money have not been completely solved, but many people are working on their solution because electronic money promises efficiencies that will reduce the costs of transactions between buyers and sellers. It will also enable access to the global

<sup>29</sup> <http://opentextbc.ca/electroniccommerce/chapter/electronic-commerce-technology/>

marketplace. In the next few years, electronic currency will displace notes and coins for many transactions.

#### **4.6.1 Electronic Funds Transfer**

Electronic funds transfer (EFT), introduced in the late 1960s, uses the existing banking structure to support a wide variety of payments. For example, consumers can establish monthly checking account deductions for utility bills, and banks can transfer millions of dollars. EFT is essentially electronic checking. Instead of writing a check and mailing it, the buyer initiates an electronic checking transaction (e.g., using a debit card at a point-of-sale terminal). The transaction is then electronically transmitted to an intermediary (usually the banking system), which transfers the funds from the buyer's account to the seller's account. A banking system has one or more common clearinghouses that facilitate the flow of funds between accounts in different banks.

Electronic checking is fast; transactions are instantaneous. Paper handling costs are substantially reduced. Bad checks are no longer a problem because the seller's account balance is verified at the moment of the transaction. EFT is flexible; it can handle high volumes of consumer and commercial transactions, both locally and internationally. The international payment clearing system, consisting of more than 100 financial institutions, handles more than one trillion dollars per day.

The major shortfall of EFT is that all transactions must pass through the banking system, which is legally required to record every transaction. This lack of privacy can have serious consequences. Cash gives anonymity.

#### **4.6.2 Digital Cash**

Digital cash is an electronic parallel of notes and coins. Two variants of digital cash are presently available: prepaid cards and smart cards. The phonecard, the most common form of prepaid card, was first issued in 1976 by the forerunner of Telecom Italia. The problem with special-purpose cards, such as phone and photocopy cards, is that people end up with a purse or wallet full of cards. A smart card combines many functions into one card. A smart card can serve as personal identification, credit card, ATM card, telephone credit card, critical medical information record and as cash for small transactions. A smart card, containing memory and a microprocessor, can store as much as 100 times more data than a magnetic-stripe card. The microprocessor can be programmed.

The stored-value card, the most common application of smart card technology, can be used to purchase a wide variety of items (e.g., fast food, parking, public transport tickets). Consumers buy cards of standard denominations (e.g., USD 50 or USD 100) from a card dispenser or bank. When the card is used to pay for an item, it must be inserted in a reader. Then, the amount of the transaction is transferred to the reader, and the value of the card is reduced by the transaction amount.

The problem with digital cash, like real cash, is that you can lose it or it can be stolen. It is not as secure as the other alternatives, but most people are likely to carry only small amounts of digital cash and thus security is not so critical. As smart cards are likely to have a unique serial number,

consumers can limit their loss by reporting a stolen or misplaced smart card to invalidate its use. Adding a PIN number to a smart card can raise its security level.

Twenty million smart cards are already in use in France, where they were introduced a decade earlier. In Austria, 2.5 million consumers carry a card that has an ATM magnetic stripe as well as a smart card chip. Stored-value cards are likely to be in widespread use in the United States within five years. Their wide-scale adoption could provide substantial benefits. Counting, moving, storing and safeguarding cash is estimated to be 4 percent of the value of all transactions. There are also significant benefits to be gained because banks don't have to hold as much cash on hand, and thus have more money available for investment.

### **4.6.3 e-cash**

Digicash of Amsterdam has developed an electronic payment system called ecash that can be used to withdraw and deposit electronic cash over the Internet. The system is designed to provide secure payment between computers using e-mail or the Internet. Ecash can be used for everyday Internet transactions, such as buying software, receiving money from parents, or paying for a pizza to be delivered. At the same time, ecash provides the privacy of cash because the payer can remain anonymous.

To use ecash, you need a digital bank account and ecash client software. The client is used to withdraw ecash from your bank account, and store it on your personal computer. You can then spend the money at any location accepting ecash or send money to someone who has an ecash account.

The security system is based on public-key cryptography and passwords. You need a password to access your account and electronic transactions are encrypted.

### **4.6.4 Credit card**

Credit cards are a safe, secure, and widely used remote payment system. Millions of people use them every day for ordering goods by phone. Furthermore, people think nothing of handing over their card to a restaurant server, who could easily find time to write down the card's details. In the case of fraud in the U.S., banks already protect consumers, who are typically liable for only the first USD 50. So, why worry about sending your credit card number over the Internet? The development of secure servers and clients has made transmitting credit card numbers extremely safe. The major shortcoming of credit cards is that they do not support person-to-person transfers and do not have the privacy of cash.

### **4.6.5 Google Wallet**

Google Wallet, now renamed as Google payment is a smart phone app released by Google in September 2011<sup>30</sup>. Google Wallet hopes to help consumers by consolidating the contents of their wallets (credit cards, debit cards and gift cards) into their phones, adding convenience and reducing clutter. Google Wallet is installed as an app that takes advantage of NFC technology, allowing consumers to pay by simply tapping their phones on a terminal. Although technically

---

<sup>30</sup> <http://sites.tufts.edu/costofcash/2013/04/11/google-wallet/>

NFC is capable of processing peer to peer transactions (for example, by bumping phones), neither Google nor its main competitor have pursued that market yet.

One difference between Google Wallet and ISIS (mobile payment network initiated by AT & T mobility, T- Mobile USA and Verizon) is in the revenue model. Whereas ISIS has aspirations of charging major credit card networks to use its ISIS system through direct fees or taking a portion of interchange, Google Wallet plans to make money by selling targeted advertisements. However, since Google Wallet and ISIS are both in early stages and currently focused on acquiring market share, no definite revenue model has been adopted yet – some reports speculate that Google Wallet may adopt a model more based on transaction fees, and others claim that they will use their relationship with Bancorp to extract an interchange fee.

#### **4.7 SUMMARY**

1. As the Internet and World Wide Web become commonly use in every household in recent years.
2. Electronic commerce, in a broad sense, is the use of computer networks to improve organizational performance.
3. E-commerce lowers the cost for people who wish to become an online merchant.
4. A modest investment in personal computer and internet connection cost can start a business online.
5. Electronic commerce is built on top of a number of different technologies. These various technologies created a layered, integrated infrastructure that permits the development and deployment of electronic commerce applications.
6. When commerce goes electronic, the means of paying for goods and services must also go electronic.
7. Any money system, real or electronic, must have a reasonable level of security and a high level of authentication, otherwise people will not use it. All
8. Consumers and organizations need to be assured that their on-line orders are protected, and organizations must be able to transfer securely many millions of dollars.
9. Electronic checking is fast; transactions are instantaneous.
10. Digital cash is an electronic parallel of notes and coins.

#### **4.8 CHECK YOUR PROGRESS**

1. \_\_\_\_\_ is the process of sharing business information, maintaining business relationships and conducting business transactions through the use of telecommunications networks.
2. Give an example of customer to customer(C2C) model.
3. There are four fundamental concerns regarding electronic money are \_\_\_\_\_, \_\_\_\_\_, \_\_\_\_\_ and \_\_\_\_\_.
4. ETF stands for \_\_\_\_\_.
5. The major shortfall of \_\_\_\_\_ is that all transactions must pass through the banking system, which is legally required to record every transaction.

6. Two variants of digital cash are presently available: \_\_\_\_\_ and \_\_\_\_\_.
7. Google wallet is now renamed as \_\_\_\_\_.

#### ***4.9 ANSWERS TO CHECK YOUR PROGRESS***

1. E-Commerce
2. eBay(Answer may vary)
3. security, authentication, anonymity, and divisibility.
4. Electronic funds transfer
5. EFT
6. prepaid cards, smart cards
7. Google Payment

#### ***4.10 MODEL QUESTIONS***

1. What is e-commerce? Name some of the famous e-commerce website.
2. List the advantages and Disadvantages of e-commerce.
3. Discuss e-commerce models in detail.
4. Explain electronic commerce infrastructure.
5. What is ecash.
6. Discuss google wallet.
7. Write a short note on ETF.
8. What is google wallet?

## **BLOCK II**

# UNIT I: INTRODUCTION TO CYBER CRIME

## 1.1 LEARNING OBJECTIVES

After going through this unit, you will be able to:

- Know the definition of cyber crime
- Classify cyber crimes
- Understand Hierarchical organizational structure of cyber criminals
- Know the reasons for commission of cyber crimes
- Define different types of malware

## 1.2 INTRODUCTION<sup>31</sup>

The term **cyber crime** is used to describe a unlawful activity in which computer or computing devices such as smartphones, tablets, Personal Digital Assistants(PDAs), etc. which are stand alone or a part of a network are used as a tool or/and target of criminal activity. It is often committed by the people of destructive and criminal mindset either for revenge, greed or adventure.

### 1.2.1 Classification of Cyber Crimes

The cyber criminal could be internal or external to the organization facing the cyber attack. Based on this fact, the cyber crime could be categorized into two types:

- 1 **Insider Attack:** An attack to the network or the computer system by some person with authorized system access is known as insider attack. It is generally performed by dissatisfied or unhappy inside employees or contractors. The motive of the insider attack could be revenge or greed. It is comparatively easy for an insider to perform a cyber attack as he is well aware of the policies, processes, IT architecture and weakness of the security system. Moreover, the attacker have an access to the network. Therefore it is comparatively easy for a insider attacker to steel sensitive information, crash the network, etc. In most of the cases the reason for insider attack is when a employee is fired or assigned new roles in an organization, and the role is not reflected in the IT policies. This opens a vulnerability window for the attacker. The insider attack could be prevented by planning and installing an Internal intrusion detection systems (IDS) in the organization.
- 2 **External Attack:** When the attacker is either hired by an insider or an external entity to the organization, it is known as external attack. The organization which is a victim of cyber attack not only faces financial loss but also the loss of reputation. Since the attacker is external to the organization, so these attackers usually scan and gathering information. An experienced network/security administrator keeps regular eye on the log

---

<sup>31</sup> This unit is adopted from “Introduction to Cyber Security” by Jeetendra Pande

generated by the firewalls as external attacks can be traced out by carefully analysing these firewall logs. Also, Intrusion Detection Systems are installed to keep an eye on external attacks.

The cyber attacks can also be classified as structure attacks and unstructured attacks based on the level of maturity of the attacker. Some of the authors have classified these attacks as a form of external attacks but there is precedence of the cases when a structured attack was performed by an internal employee. This happens in the case when the competitor company wants the future strategy of an organization on certain points. The attacker may strategically gain access to the company as an employee and access the required information.

- *Unstructured attacks:* These attacks are generally performed by amateurs who don't have any predefined motives to perform the cyber attack. Usually these amateurs try to test a tool readily available over the internet on the network of a random company.
- *Structure Attack:* These types of attacks are performed by highly skilled and experienced people and the motives of these attacks are clear in their mind. They have access to sophisticated tools and technologies to gain access to other networks without being noticed by their Intrusion Detection Systems (IDSs). Moreover, these attackers have the necessary expertise to develop or modify the existing tools to satisfy their purpose. These types of attacks are usually performed by professional criminals, by a country on other rival countries, politicians to damage the image of the rival person or the country, terrorists, rival companies, etc.

### 1.2.2 Reasons for Commission of Cyber Crimes

There are many reasons which act as a catalyst in the growth of cyber crime. Some of the prominent reasons are:

- a. *Money:* People are motivated towards committing cyber crime is to make quick and easy money.
- b. *Revenge:* Some people try to take revenge with other person/organization/society/ caste or religion by defaming its reputation or bringing economical or physical loss. This comes under the category of cyber terrorism.
- c. *Fun:* The amateur do cyber crime for fun. They just want to test the latest tool they have encountered.
- d. *Recognition:* It is considered to be pride if someone hack the highly secured networks like defense sites or networks.
- e. *Anonymity:* Many time the anonymity that a cyber space provide motivates the person to commit cyber crime as it is much easy to commit a cyber crime over the cyber space and remain anonymous as compared to real world.

It is much easier to get away with criminal activity in a cyber world than in the real world. There is a strong sense of anonymity than can draw otherwise respectable citizens to abandon their ethics in pursuit personal gain.



- f. **Cyber Espionage:** At times the government itself is involved in cyber trespassing to keep eye on other person/network/country. The reason could be politically, economically socially motivated.

### 1.3 MALWARE AND ITS TYPES

Malware stands for “*Malicious Software*” and it is designed to gain access or installed into the computer without the consent of the user. They perform unwanted tasks in the host computer for the benefit of a third party. There is a full range of malwares which can seriously degrade the performance of the host machine. There is a full range of malwares which are simply written to distract/annoy the user, to the complex ones which captures the sensitive data from the host machine and send it to remote servers. There are various types of malwares present in the Internet. Some of the popular ones are:

#### 1.3.1 Adware

It is a special type of malware which is used for forced advertising. They either redirect the page to some advertising page or pop-up an additional page which promotes some product or event. These adware are financially supported by the organizations whose products are advertised.



Figure 14: Adware<sup>32</sup>

#### 1.3.2 Spyware

It is a special type of which is installed in the target computer with or without the user permission and is designed to steal sensitive information from the target machine. Mostly it gathers the browsing habits of the user and the send it to the remote server without the

<sup>32</sup> Image courtesy: [www.howtouninstallmalware.com](http://www.howtouninstallmalware.com)

knowledge of the owner of the computer. Most of the time they are downloaded in to the host computer while downloading freeware i.e. free application programmes from the internet. Spywares may be of various types; It can keeps track of the cookies of the host computer, it can act as a keyloggers to sniff the banking passwords and sensitive information, etc.



Figure 15: Spyware<sup>33</sup>

### 1.3.3 Browser hijacking software

There are some malicious software which are downloaded along with the free software offered over the internet and installed in the host computer without the knowledge of the user. This software modifies the browsers setting and redirect links to other unintentional sites.

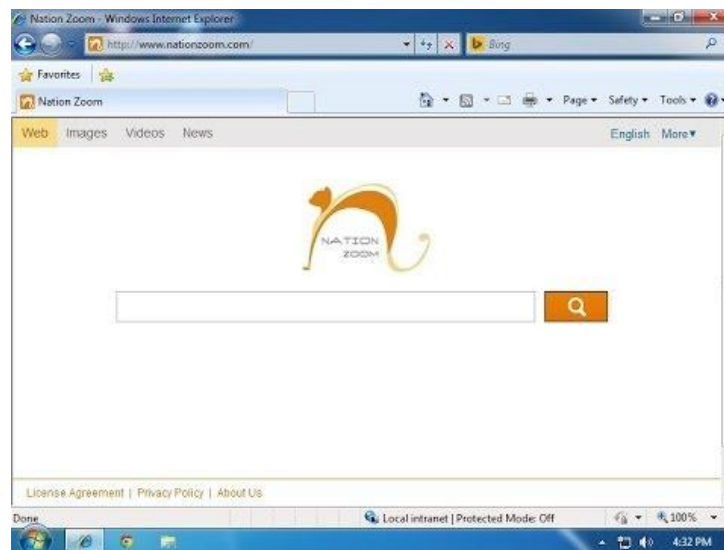


Figure 16: Browser hijacking<sup>34</sup>

<sup>33</sup> Image courtesy: [https://c1.staticflickr.com/1/112/284537362\\_e29b9601c6.jpg](https://c1.staticflickr.com/1/112/284537362_e29b9601c6.jpg)

<sup>34</sup> Image courtesy: <https://i.ytimg.com/vi/CzEhMRSeTPo/hqdefault.jpg>

### 1.3.4 Virus

A virus is a malicious code written to damage/harm the host computer by deleting or appending a file, occupy memory space of the computer by replicating the copy of the code, slow down the performance of the computer, format the host machine, etc. It can be spread via email attachment, pen drives, digital images, e-greeting, audio or video clips, etc. A virus may be present in a computer but it cannot activate itself without the human intervention. Until and unless the executable file(.exe) is execute, a virus cannot be activated in the host machine.

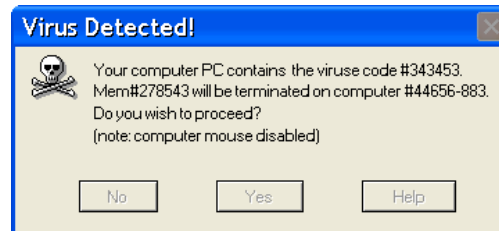


Figure 17: Computer virus<sup>35</sup>

### 1.3.5 Worms

They are a class of virus which can replicate themselves. They are different from the virus by the fact that they does not require human intervention to travel over the network and spread from the infected machine to the whole network. Worms can spread either through network, using the loopholes of the Operating System or via email. The replication and spreading of the worm over the network consumes the network resources like space and bandwidth and force the network to choke. It is a program that views the infection point as another computer rather than as other executable files on an already infected computer<sup>36</sup>. In simplistic terms this normally means when infected you will only have a single infected program on your computer rather than thousands of the programs you have installed being infected. A worm is much more sneaky at infecting a computer, but thankfully they are also much easier to identify once infected. The reason they are considered to be more sneaky is because a worm has many more tools at its disposal that it can use to infect you than a virus has. They not only use infected files to lure you, but they take advantage of the fact that programs have bugs that allow them to wiggle into your computer. This means that a worm can infect your computer without you ever having to execute a program infected with a worm, instead they can gain entrance through an open communications port on your computer (which is a virtual port that has no physical self). An important note though is that worms, like viruses, still are required to be executed in order to infect your machine. However, the difference is that worms not only can trick you into infecting yourself, but they can trick your computer into thinking you want to execute them.

<sup>35</sup> Image courtesy: <http://atom.smasher.org/> © Atom Smasher and available under your choice of Creative Commons Attribution-Share Alike 3.0 License

<sup>36</sup> <https://itgs-417.wikispaces.com/16.-+Worms>

Once you are infected with a worm then your computer becomes a zombie that attempts to infect other computers, normally without you ever knowing anything ever happened. Thankfully the majority of worms are written by very poor programmers with little want more than to make a statement to the world. For this reason worms are rarely destructive from a permanent perspective and often are not anywhere as successful as they should be if they were written properly.

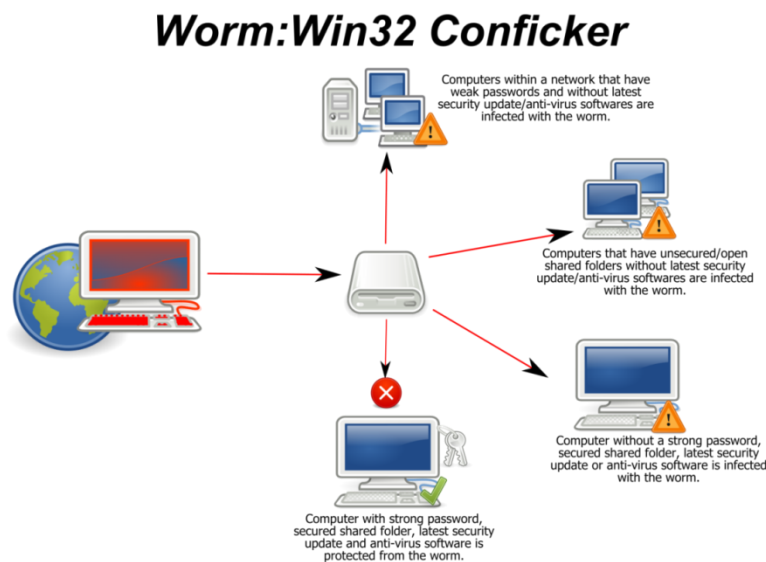


Figure 18: An example of a Computer worm- Conficker<sup>37</sup>

### 1.3.6 Trojan Horse

A Trojan virus is a piece of software designed to look like a useful file or software program but performs a possibly nefarious function once installed on a client computer. The virus takes its name from the “Trojan Horse” from Greek mythology setup outside of the city of Troy. Trojan horse viruses differ from other computer viruses in that they are not designed to spread themselves. Instead Trojan horse malware is either delivered as the payload of another virus or piece of malware or through manual end-user action by downloading infected files or inserting infected drives into a computer. Once a computer is infected with a Trojan virus, the malware can be designed to steal end-user information, perform destructive harm on the target computer, or even download additional computer malware. A Trojan virus will normally consist of a server and client component. The client component is the portion of the malware that infects the end-user’s computer. Once established or executed, the virus can be designed to establish a certain level of control over the infected computer.

It not only damages the host computer by manipulating the data but also it creates a backdoor in the host computer so that it could be controlled by a remote computer.

<sup>37</sup> Image courtesy: <https://upload.wikimedia.org/wikipedia/commons/thumb/5/53/Conficker.svg/2000px-Conficker.svg.png>



Figure 19: Working of a Trojan horse

It can become a part of *botnet*(robot-network), a network of computers which are infected by malicious code and controlled by central controller. The computers of this network which are infected by malicious code are known as zombies. Trojens neither infect the other computers in the network nor do they replicate.

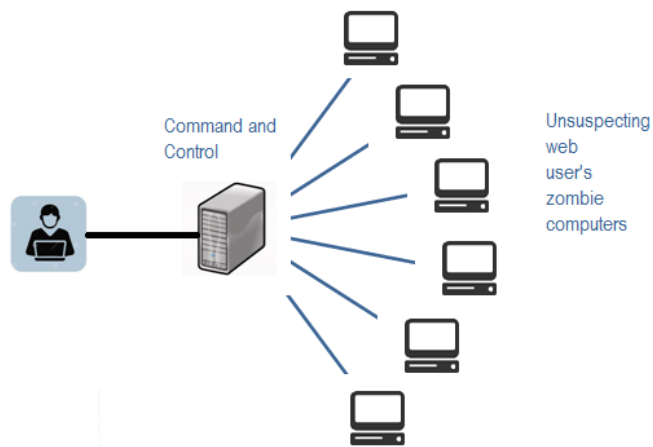


Figure 20: A typical botnet



The categories currently used to define the different variants of Trojan viruses include:

- **Remote access:** virus will give the hacker/attacker full control over the targeted computer equivalent to the user's permissions.
- **Password sending:** the malware will search for all cached passwords and copy those that are entered by the end-user.
- **Destructive:** A destructive Trojan virus's primary purpose is to delete or remove files on the targeted computer.
- **Key loggers:** are a variant of Trojan virus that is designed to record the keystrokes on an infected computer and then send the log files to a remote server or email account.
- **Denial of service:** A denial of service (DoS) attack Trojan virus will be designed to use the infected computer as a bot to attack another web server or computer. Combined with other computers that are infected, the Internet connection for the attacked computer can become too busy to allow regular users to make use of the site.
- **Proxy:** A proxy or Wingate Trojan virus is designed to make the infected computer act as a Wingate or proxy server. As a result of the infection, the targeted computer can then be used by other to surf the Internet in an anonymous fashion.
- **FTP:** A FTP Trojan virus is one of the most basic Trojan viruses in the wild and is one of the most outdated. The primary purpose of the malware is to open port 21 on the infected computer. Once opened, anyone can then connect to the computer using the FTP protocol.
- **Software detection killers:** The purpose of this variant of Trojan virus is to disable known antivirus and computer firewall programs.
- **Trojan down loaders:** The sole job that a Trojan downloader does on the infected computer is to download additional computer malware onto the infected computer.

### 1.3.7 Scareware

Internet has changed how we talk, shop, play etc. It has even changed the way how the criminal target the people for ransom. While surfing the Internet, suddenly a pop-up alert appears in the screen which warns the presence of dangerous virus, spywares, etc. in the user's computer.



Figure 21: Scareware

As a remedial measure, the message suggests the user to download the full paid version of the software. As the user proceeds to download, a malicious code, known as scareware is downloaded into the host computer. It holds the host computer hostage until the ransom is paid. The malicious code can neither be uninstalled nor can the computer be used till the ransom is paid. A sample message alert of a scareware is shown below in Figure 36<sup>38</sup>.

## 1.4 SUMMARY

- 1 The term cyber crime is used to describe a unlawful activity in which computer or computing devices such as smartphones, tablets, Personal Digital Assistants(PDAs), etc. which are stand alone or a part of a network are used as a tool or/and target of criminal activity.
- 2 The cyber criminal could be internal or external to the organization facing the cyber attack.
- 3 An attack to the network or the computer system by some person with authorized system access is known as insider attack.
- 4 Structure attack are performed by highly skilled and experienced people and the motives of these attacks are clear in their mind.
- 5 When the attacker is either hired by an insider or an external entity to the organization, it is known as external attack.
- 6 There are some cyber criminals offers on-demand and service.
- 7 Malware stands for “*Malicious Software*” and it is designed to gain access or installed into the computer without the consent of the user.
- 8 Spyware is a special type of which is installed in the target computer with or without the user permission and is designed to steal sensitive information from the target machine.

## 1.5 CHECK YOUR PROGRESS

Fill In the Blanks

- 1 \_\_\_\_\_ are generally performed by dissatisfied or unhappy inside employees or contractors.
- 2 \_\_\_\_\_ are installed to keep an eye on external attacks.
- 3 \_\_\_\_\_ are generally performed by amateurs who don't have any predefined motives to perform the cyber attack.
- 4 Malware stands for \_\_\_\_\_ .
- 5 \_\_\_\_\_ is a malicious code that is installed in the host machine by pretending to be useful software.

---

<sup>38</sup> Image courtesy: <https://www.flickr.com/photos/alamagordo/2372928527>

- 6 \_\_\_\_\_ is a special type of malware which is used for forced advertising.
- 7 BotNet stands for \_\_\_\_\_ .

## ***1.6 ANSWERS TO CHECK YOUR PROGRESS***

- 1 Insider attacks
- 2 Intrusion Detection Systems
- 3 Unstructured
- 4 Malicious Software
- 5 Trojan horse
- 6 Adware
- 7 Robot Network

## ***1.7 MODEL QUESTIONS***

1. What is a cyber crime? Define.
2. Classify cyber crimes.
3. Define the Organizational hierarchical structure of cyber criminals.
4. What are the various types of motivations that lure the people for cyber crime?
5. What is cyber espionage?
6. What is a malware? What are different types of malwares?
7. What is Virus? How does it harm a computer?
8. What is the difference between a worm and a virus?
9. What is a scareware?
10. What is the difference between structured and unstructured cyber attacks?



## UNIT II: KINDS OF CYBER CRIME

### 2.1 LEARNING OBJECTIVES

After going through this unit, you will be able to:

- Know different types of cyber crime
- Understand cyber stalking
- Define software piracy and crime related to IPRs
- Classify different types of hackers
- Know spamming
- Understand cross site scripting
- Know online auction frauds
- Know cyber squatting
- Understand web jacking
- Understand Denial of Service attack

### 2.2 KINDS OF CYBER CRIME

This section describes various types of cyber crimes. Some of the important ones are:

#### 2.2.1 Cyber Stalking

It is an act of stalking, harassing or threatening someone using Internet/computer as a medium. This is often done to defame a person and use email, social network, instant messenger, web-posting, etc. as a using Internet as a medium as it offers anonymity. The behavior includes false accusations, threats, sexual exploitation to minors, monitoring, etc.

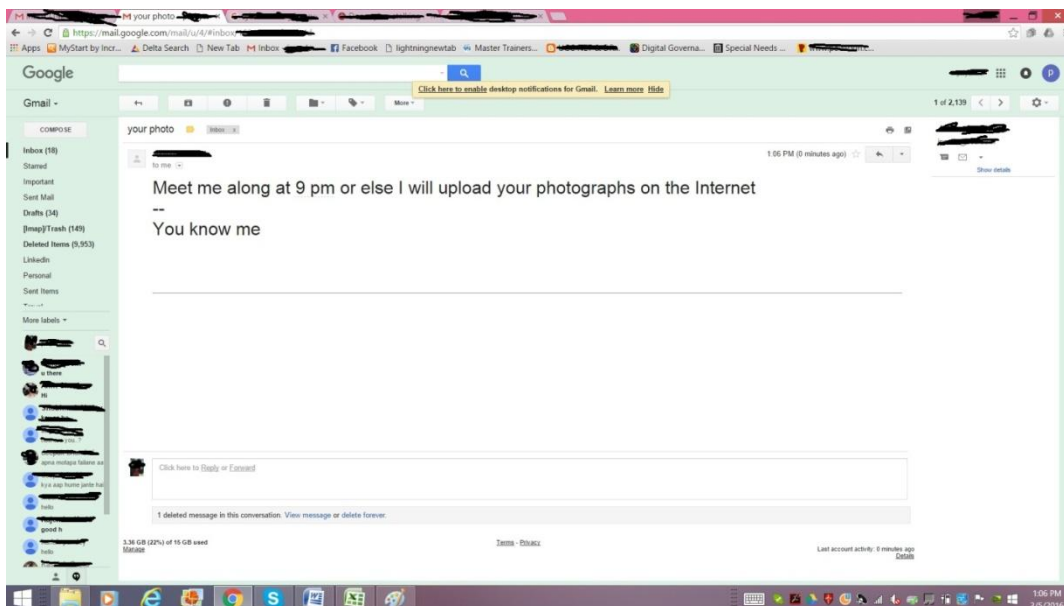


Figure 22: Sample stalking email

### 2.2.2 Child Pornography

It is an act of possessing image or video of a minor (under 18), engaged in sexual conduct. Nowadays, internet use and access is becoming increasingly common as a great entertainment, communication and educational resource for children as well as for adults<sup>39</sup>. Internet is a perfect environment for children, for exploring the world, learning and having fun. However, accesses to illegal sites that contain violence and sexuality, and contact dangerous people are among the particular risks for children using the internet. It is a known fact that, internet and developing technology make the production and distribution of child pornography cheaper and easier.

### 2.2.3 Forgery and Counterfeiting

It is a use of computer to forgery and counterfeiting is a document. With the advancement in the hardware and the software, it is possible to produce counterfeit which matches the original document to such an extent that it is not possible to judge the authenticity of the document without expert judgment.



Figure 23: Forgery and counterfeiting using computer<sup>40</sup>

### 2.2.4 Software Piracy and Crime related to IPRs

Software piracy is an illegal reproduction and distribution for personal use or business. It comes under crime related to IPR infringement. Some of the other crimes under IPR infringement are: download of songs, downloading movies, etc.

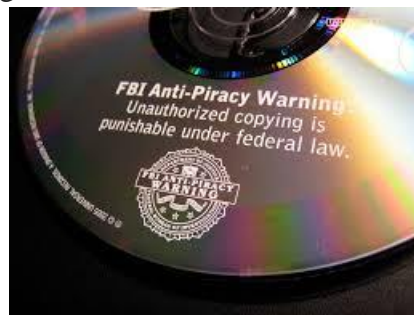


Figure 24: FBI warning for anti software piracy<sup>41</sup>

<sup>39</sup> <https://www.j-humansciences.com/ojs/index.php/IJHS/article/view/887/528>

<sup>40</sup> Image courtesy: <https://upload.wikimedia.org/wikipedia/commons/f/f1/Forgery%2BGenuinePuertoPrincipe-1899.jpg>

## 2.2.5 Cyber Terrorism

It is defined as the use of computer resources to intimidate or coerce government, the civilian population or any segment thereof in furtherance of political or social objectives. It is the act of Internet terrorism in terrorist activities, including acts of deliberate, large-scale disruption of computer networks, especially of personal computers attached to the Internet, by the means of tools such as computer viruses<sup>42</sup>. Cyberterrorism can be also defined as the intentional use of computer, networks, and public internet to cause destruction and harm for personal objectives. Objectives may be political or ideological since this can be seen as a form of terrorism.

## 2.2.6 Phishing

It is a process of acquiring personal and sensitive information of an individual via email by disguising as a trustworthy entity in an electronic communication. The purpose of phishing is identity theft and the personal information like username, password, and credit card number etc. may be used to steal money from user account. If a telephone is used as a medium for identity theft, it is known as *Vishing* (voice phishing). Another form of phishing is *Smishing*, in which sms is used to lure customers.

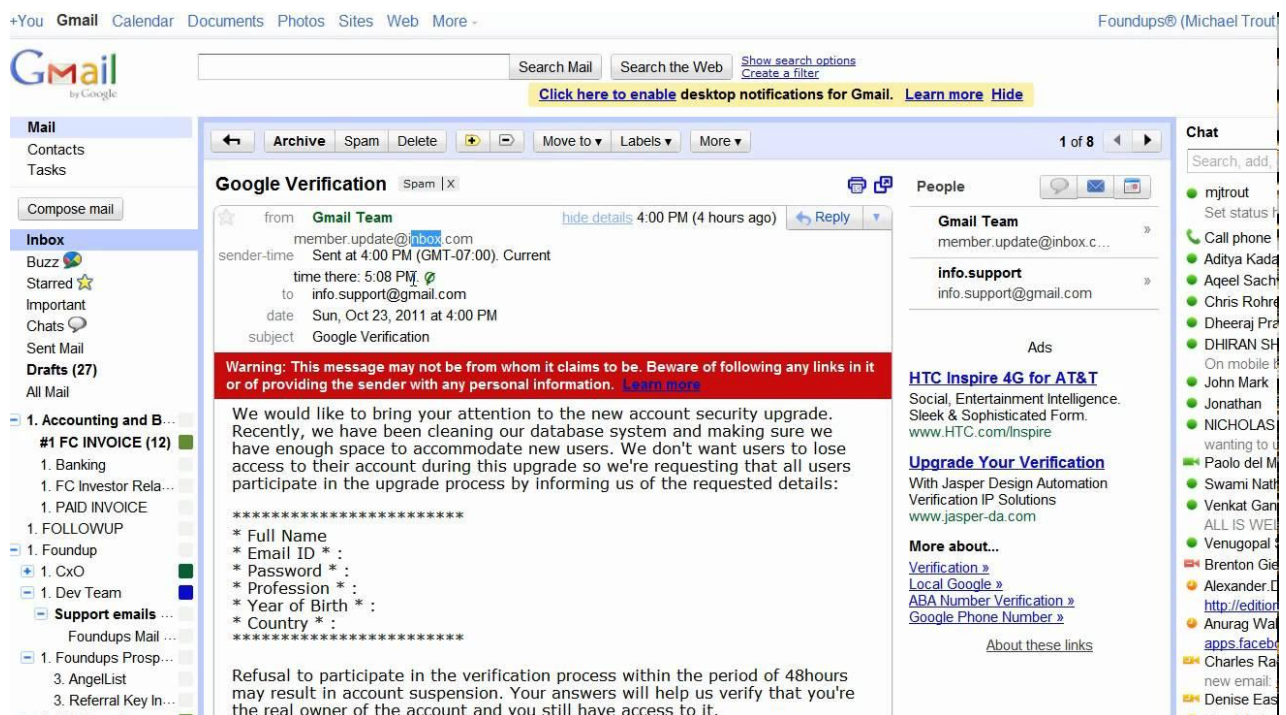


Figure 25: Phishing<sup>43</sup>

<sup>41</sup> Image courtesy: [https://upload.wikimedia.org/wikipedia/commons/8/81/Fbi\\_anti\\_piracy\\_warning.jpg](https://upload.wikimedia.org/wikipedia/commons/8/81/Fbi_anti_piracy_warning.jpg)

<sup>42</sup> <https://en.wikipedia.org/wiki/Cyberterrorism>

<sup>43</sup> Image courtesy: <https://i.ytimg.com/vi/0NuV2jvdVw4/maxresdefault.jpg>

### 2.2.7 Computer Vandalism

**Vandalism** is action involving deliberate destruction of or damage to public or private property<sup>44</sup>. The term also includes criminal damage such as graffiti and defacement directed towards any property without permission of the owner. The term finds its roots in an Enlightenment view that the Germanic Vandals were a uniquely destructive people. Computer Vandalism is an act of physical destroying computing resources using physical force or malicious code.



*Figure 26: Broken computer screen due to the act of vandalism<sup>45</sup>*

### 2.2.8 Computer Hacking

It is a practice of modifying computer hardware and software to accomplish a goal outside the creator's original purpose. The purpose of hacking a computer system may vary from simply demonstrations of the technical ability, to sealing, modifying or destroying information for social, economic or political reasons. Now the corporate are hiring hackers, a person who is engaged in hacking computers, to intentionally hack the computer of an organization to find and fix security vulnerabilities. The hackers may be classified as:

- **White Hat:** white hat hackers are the persons who hack the system to find the security vulnerabilities of a system and notify to the organizations so that a preventive action can be taken to protect the system from outside hackers. White hat hackers may be paid employee of an organization who is employed to find the security loop-holes, or may be a freelancer who just wants to prove his mantle in this field. They are popular known as ethical hackers.
- **Black Hat:** in contrast to the white hat, the black hat hack the system with ill intentions. They may hack the system for social, political or economically motivated intentions.

<sup>44</sup> <https://en.wikipedia.org/wiki/Vandalism>

<sup>45</sup> Image courtesy: <https://upload.wikimedia.org/wikipedia/commons/9/9d/Brokenlaptop.png>

They find the security loopholes the system, and keep the information themselves and exploit the system for personal or organizational benefits till organization whose system is compromised is aware of this, and apply security patches. They are popularly known as crackers.

- Grey Hat: Grey hat hackers find out the security vulnerabilities and report to the site administrators and offer the fix of the security bug for a consultancy fee.
- Blue hat: A blue hat hacker is someone outside computer security consulting firms who is used to bug-test a system prior to its launch, looking for exploits so they can be closed.

### 2.2.9 Creating and distributing viruses over internet

A Computer virus<sup>46</sup> is a parasitic program written intentionally to enter a computer without the users permission or knowledge. The word parasite is used because a virus attaches to files or boot sectors and replicates itself, thus continuing to spread. Though some virus's do little but replicate others can cause serious damage or effect program and system performance. A virus should never be assumed harmless and left on a system—Symantec. Five most common types:

- 1 Macro virus - this type of virus usually comes as part of a document or spreadsheet, often in email.
- 2 Boot sector virus - this type of virus overwrites the boot sector on your hard drive or floppy drive.
- 3 File infector virus - this type of virus attaches itself to executables, for example .com and .exe files.
- 4 Stealth virus - this type of virus tries to fool antivirus software by catching its requests to the operating system (asking to open a file, for example).
- 5 Self-modifying virus - this type of virus was designed to avoid detection by antivirus software by changing itself internally.

The spreading of a virus can cause business and financial loss to an organization. The loss includes the cost of repairing the system, cost associated with the loss of business during downtime and cost of loss of opportunity. The organization can sue the hacker, if found, for the sum of more than or equivalent to the loss borne by the organization.

### 2.2.10 Spamming

Sending of unsolicited and commercial bulk message over the internet is known as spamming. An email can be classified as spam, if it meets following criteria:

- a. Mass mailing:- the email is not targeted to one particular person but to a large number of peoples.
- b. Anonymity:- The real identify of the person not known.
- c. Unsolicited:- the email is neither expected nor requested for the recipient.

These spams not only irritate the recipients and overload the network but also waste the time and occupy the valuable memory space of the mailbox.

---

<sup>46</sup> <https://itgs-417.wikispaces.com/14.-+Virus>



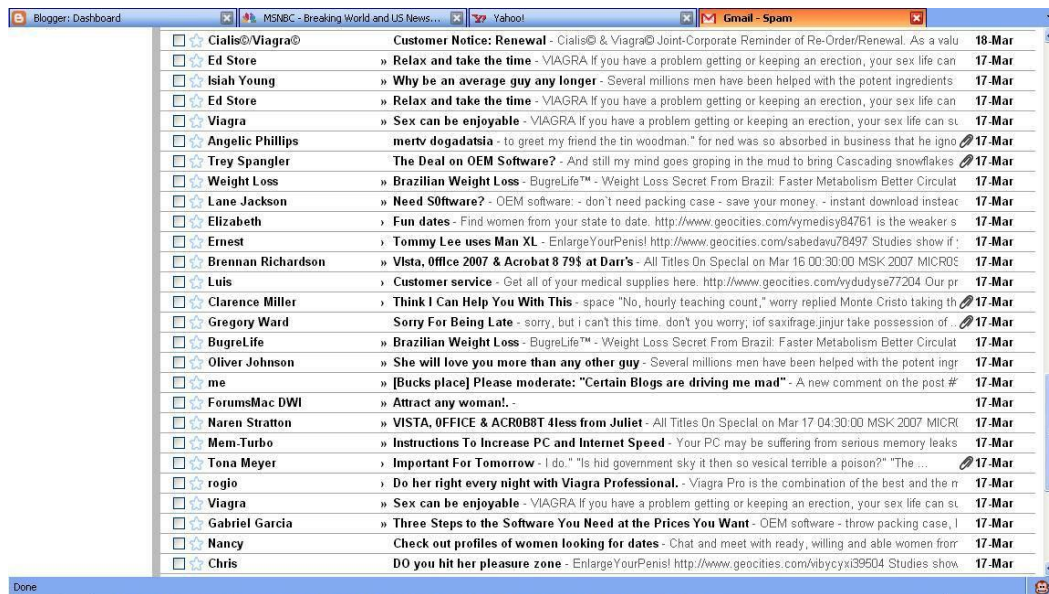


Figure 27: Spam mail<sup>47</sup>

### 2.2.11 Cross Site Scripting

It is an activity which involves injecting a malicious client side script into a trusted website. As soon as the browser executes the malicious script, the malicious script gets access to the cookies and other sensitive information and sent to remote servers. Now this information can be used to gain financial benefit or physical access to a system for personal interest.

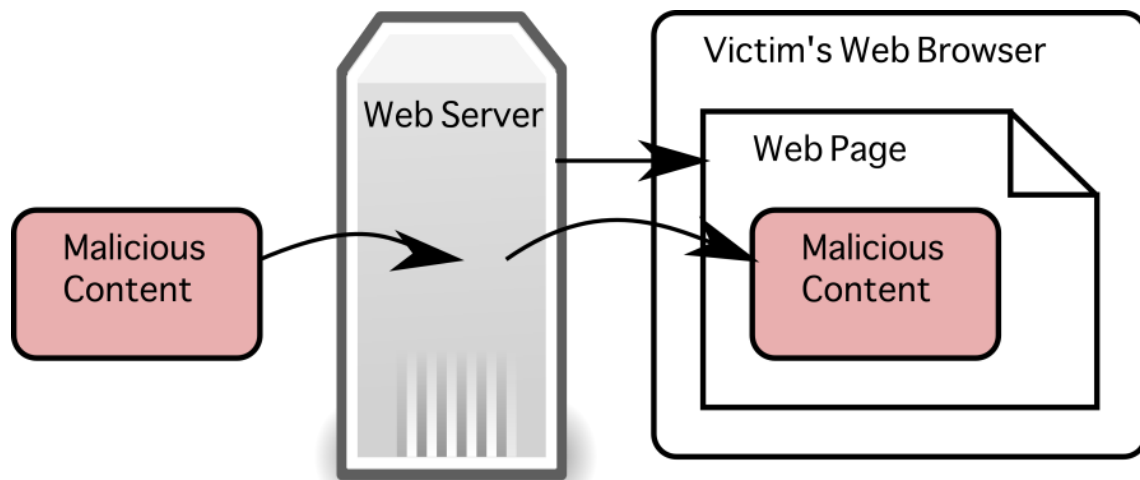


Figure 28: Cross site scripting process<sup>48</sup>

<sup>47</sup> Image courtesy: <http://thewhizzer.blogspot.in/2007/03/e-mail-spam-and-general-whinge.html> available under creative commons license.

<sup>48</sup> Image courtesy: <https://www.flickr.com/photos/terrio/5710831966>

## 2.2.12 Online Auction Fraud

There are many genuine websites who offers online auction over internet. Taking the advantage of the reputation of these websites, some of the cyber criminals lure the customers to online auction fraud schemes which often lead to either overpayment of the product or the item is never delivered once the payment is made.

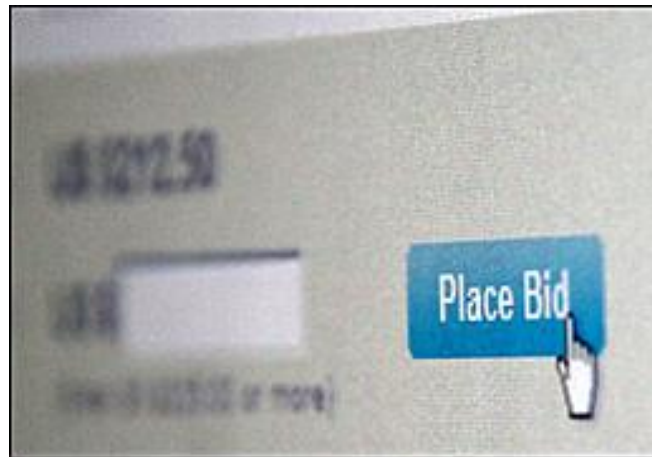


Figure 29: Online bidding<sup>49</sup>

## 2.2.13 Cyber Squatting

It is an act of reserving the domain names of someone else's trademark with intent to sell it afterwards to the organization who is the owner of the trademark at a higher price.

The screenshot shows the Godaddy website interface. At the top, there is a navigation menu with links for 'All Products', 'Domains', 'Websites', 'Hosting', 'Web Security', 'Online Marketing', and 'Email & Office'. There are also links for 'Coupons' and 'GoDaddy Pro'. A search bar contains the text 'orangenetwork'. To the right of the search bar are buttons for 'SEARCH AGAIN' and 'CONTINUE TO CART'. Below the search bar, a message states: 'Sorry, **orangenetwork.com** isn't available.' Underneath this message, it says 'GET ANY OF THESE RELATED DOMAINS FOR Rs 99.00'. A table lists three related domains with their original prices (Rs 959.00) and current sale prices (Rs 99.00), each with a 'SELECT' button.

Domain Name	Original Price	Current Price	Action
orangenetworkweb.com	Rs 959.00	Rs 99.00*	SELECT
orangenetworkpro.com	Rs 959.00	Rs 99.00*	SELECT
orangenetworkhub.com	Rs 959.00	Rs 99.00*	SELECT

Figure 30: Cyber squatting

<sup>49</sup> Image courtesy: [https://www.fbi.gov/news/stories/2009/june/auctionfraud\\_063009](https://www.fbi.gov/news/stories/2009/june/auctionfraud_063009)

### 2.2.14 Logic Bombs

In a computer program, a logic bomb<sup>50</sup>, also called slag code (because all that's left after it detonates is computer slag), is programming code, inserted surreptitiously or intentionally, that is designed to execute (or "explode") under circumstances. For example, a programmer may hide a piece of code that starts deleting files (such as a salary database trigger), should they ever be terminated from the company. To be considered a logic bomb, the payload should be unwanted and unknown to the user of the software.

It's secretly inserted into the code of a computer's existing software, where it lies dormant until that event occurs. This event might be a positive trigger, such as a specific date. Trojans that activate on certain dates are often called "time bombs". Negative triggers are considered to be more dangerous than positive ones, since the risk of accidentally triggering the bomb increases dramatically.

A logic bomb could also be programmed to wait for a certain message from the programmer. The logic bomb could, for example, check a web site once a week for a certain message. When the logic bomb sees that message, or when the logic bomb stops seeing that message, it activates and executes its code. A logic bomb, when "exploded," may be designed to display or print a spurious message, delete or corrupt data, or have other undesirable effects. Because a logic bomb does not replicate itself, it is very easy to write a logic bomb program. This also means that a logic bomb will not spread to unintended victims. In some ways, a logic bomb is the most civilized programmed threat, because a logic bomb must be targeted against a specific victim.

### 2.2.15 Internet Time Thefts

Hacking the username and password of ISP of an individual and surfing the internet at his cost is Internet Time Theft.

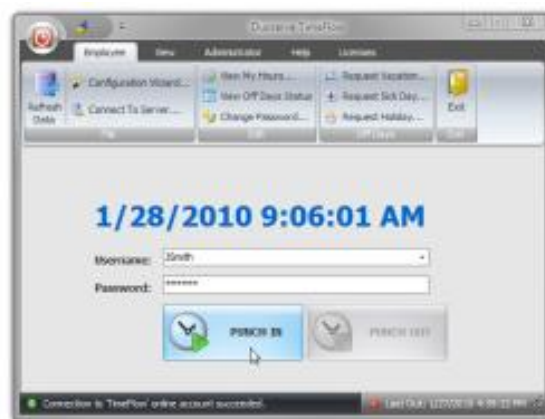


Figure 31: Stealing other's username and password for internet access<sup>51</sup>

<sup>50</sup> <https://itgs-417.wikispaces.com/17.-+Logic+Bombs>

<sup>51</sup> Image courtesy: [http://i.i.cbsi.com/cnwk.1d/i/tim//2010/04/08/7418d12f4a1d0a0f8beb7c10836f328c363b\\_1time\\_clock\\_software\\_640x480\\_257x193.jpg](http://i.i.cbsi.com/cnwk.1d/i/tim//2010/04/08/7418d12f4a1d0a0f8beb7c10836f328c363b_1time_clock_software_640x480_257x193.jpg)



### 2.2.16 Web Jacking

The hacker gain access to a website of an organization and either blocks it or modify it to serve political, economical or social interest. The recent examples of web jacking are some of the websites of the educational institutes were hacked by Pakistani hackers and an animation which contains Pakistani flags were flashed in the homepage of these websites. Another example is Indian hackers hacked website of Pakistani railways and flashed Indian flag in the homepage for several hours on the occasion of Independence Day of India in 2014.

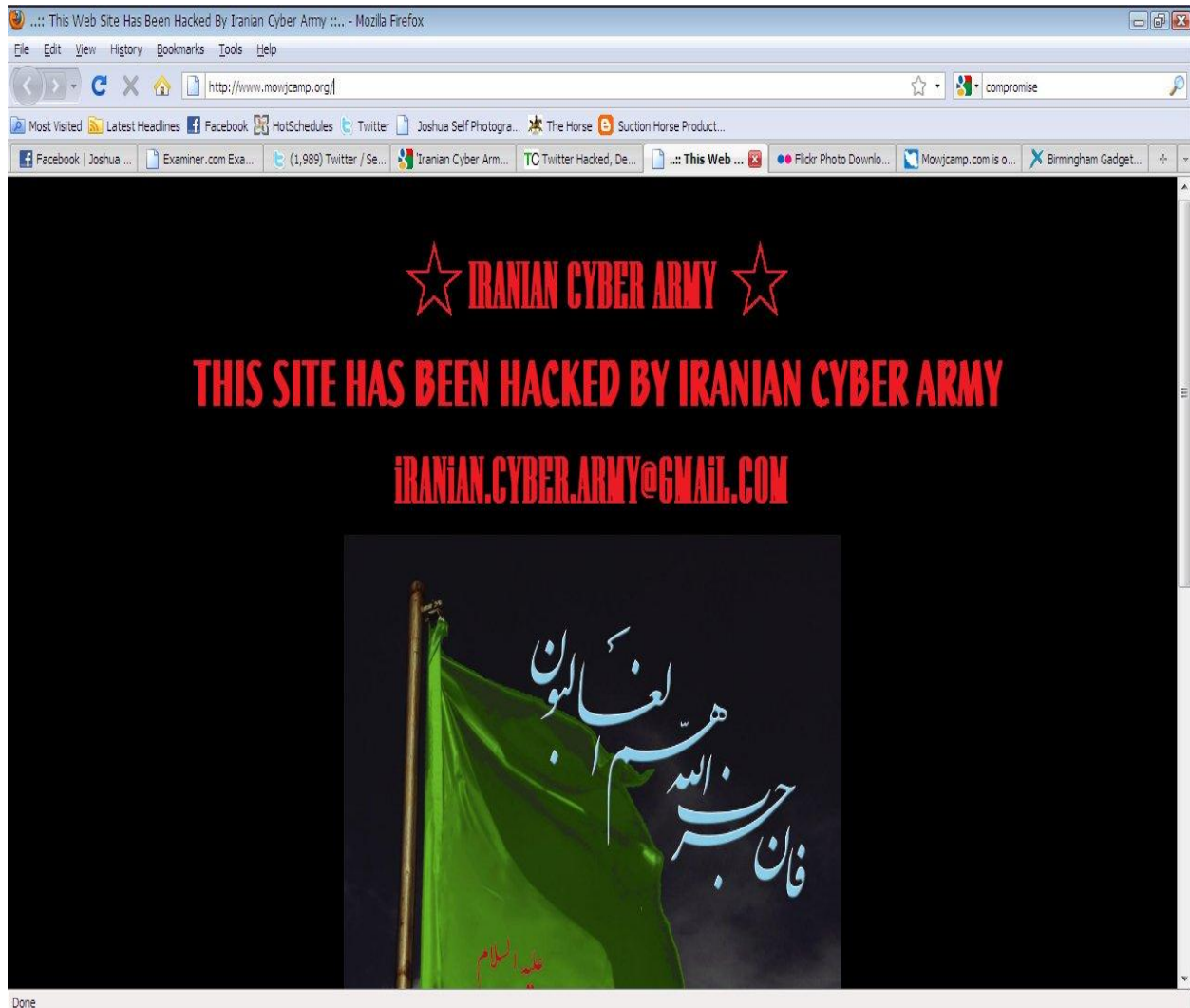


Figure 32: Web jacking by Iranian hackers<sup>52</sup>

### 2.2.17 Denial of Service Attack

It is a cyber attack in which the network is choked and often collapsed by flooding it with useless traffic and thus preventing the legitimate network traffic.

<sup>52</sup> Image courtesy: <https://www.flickr.com/photos/xabbu/4194772244>

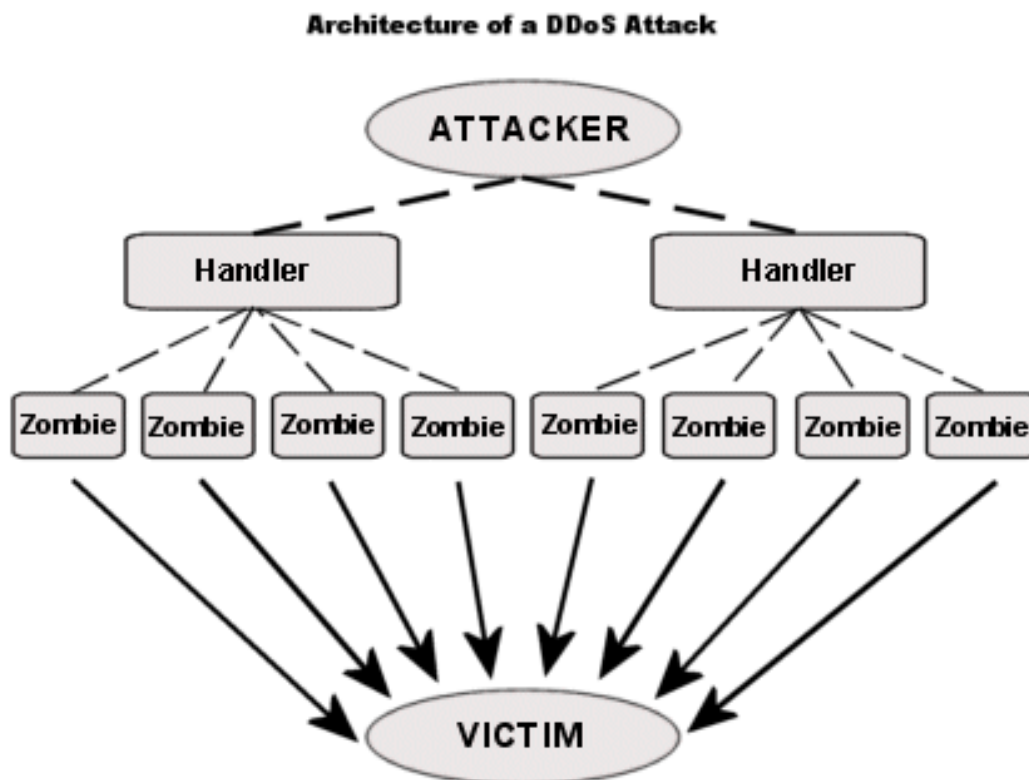


Figure 33: Denial of Service attack<sup>53</sup>

### 2.2.18 Salami Attack

It is an attack which proceeds with small increments and final add up to lead to a major attack. The increments are so small that they remain unnoticed. An example of salami attack is gaining access to online banking of an individual and withdrawing amount in such a small amounts that it remains unnoticed by the owner. Often there is default trigger set in the banking website and transactions below say, Rs. 1000 withdrawal are not reported to the owner of the account. Withdrawing amount of Rs. 1000 over a period of time will lead to total withdrawal of a large sum.

### 2.2.19 Data Diddling

It is a practice of changing the data before its entry into the computer system. Often, the original data is retained after the execution on the data is done. For example, DA or the basic salary of the person is changed in the payroll data of an individual for pay calculation. Once the salary is calculated and transferred to his account, the total salary is replaced by his actual salary in the report. The example below shows how Employee number were switched so overtime was credited to wrong employee.

<sup>53</sup> Image courtesy: [https://upload.wikimedia.org/wikipedia/commons/e/e8/Denial-of-service\\_attack.gif](https://upload.wikimedia.org/wikipedia/commons/e/e8/Denial-of-service_attack.gif)

Timekeeper			Payroll		
Emp Code	Name	Work Hrs	Emp Code	Work Hrs	Salary
1234	XYZ	45	1234	45	45832
1235	ABC	54	1235	50	50354
1236	MNO	50	1236	54	55963

Figure 34: Example of data diddling

### 2.2.20 Email Spoofing

It is a process of changing the header information of an e-mail so that its original source is not identified and it appears to an individual at the receiving end that the email has been originated from source other than the original source.

Previous | [Next](#) | [Back to Messages](#) [Mark as Unread](#) | [Print](#)

Delete Reply Forward Spam Move...

**RE: Job Proposal** Saturday, 15 January, 2011 4:18 PM  
 From: "Rjt roy" <rjtroy@live.com>  
 To: "my yahoo id" <rjtroy@ymail.com>

Hello **Mr. Bill Gates**

it's like my dream come true ,you offering me job in Microsoft corporation , it is my pleasure to accept your offer .  
 please email me the other details, so i can join company soon .

Awaiting reply  
**Thanks & regard**  
**Rohit Chohan**

---

To: rjtroy@live.com  
 Subject: Job Proposal  
 From: bill\_gates@microsoft.com  
 Date: Sat, 15 Jan 2011 17:10:53 +0100

**Hello Rohit,**  
**I'm Bill Gates from Microsoft corporation,yesterday my Secretary forward your resume to me , we saw it was fullfil our requirement on company , it's Job Proposal to you for to be a CEO of Microsoft Corporation !!!**

Awaiting reply  
**Thanks & regard**  
**Bill Gates**

Delete Reply Forward Spam Move...

Figure 35: Example of email spoofing<sup>54</sup>

<sup>54</sup> <http://s1216.photobucket.com/user/rjtheindian/media/emailspoofing3.png.html>

## 2.3 SUMMARY

1. Cyber stacking is an act of stalking, harassing or threatening someone using Internet/computer as a medium.
2. With the advancement in the hardware and the software, it is possible to produce counterfeit which matches the original document to such an extent that it is not possible to judge the authenticity of the document without expert judgment.
3. Hacking is a practice of modifying computer hardware and software to accomplish a goal outside the creator's original purpose.
4. The spreading of a virus can cause business and financial loss to an organization.
5. The hacker gain access to a website of an organization and either blocks it or modify it to serve political, economical or social interest.
6. Salami attack is an attack which proceeds with small increments and final add up to lead to a major attack. The increments are so small that they remain unnoticed.

## 2.4 CHECK YOUR PROGRESS

1. \_\_\_\_\_ often done to defame a person and use email, social network, instant messenger, web-posting, etc. as a using Internet as a medium as it offers anonymity. The behavior includes false accusations, threats, sexual exploitation to minors, monitoring, etc.
2. \_\_\_\_\_ is an act of possessing image or video of a minor (under 18), engaged in sexual conduct.
3. \_\_\_\_\_ is an illegal reproduction and distribution for personal use or business.
4. If a telephone is used as a medium for identity theft, it is known as \_\_\_\_\_.
5. \_\_\_\_\_ hackers are the persons who hack the system to find the security vulnerabilities of a system and notify to the organizations so that a preventive action can be taken to protect the system from outside hackers.
6. A \_\_\_\_\_ hacker is someone outside computer security consulting firms who is used to bug-test a system prior to its launch, looking for exploits so they can be closed.
7. \_\_\_\_\_ is an act of reserving the domain names of someone else's trademark with intent to sell it afterwards to the organization who is the owner of the trademark at a higher price.
8. \_\_\_\_\_ is a cyber attack in which the network is choked and often collapsed by flooding it with useless traffic and thus preventing the legitimate network traffic.
9. \_\_\_\_\_ virus usually comes as part of a document or spreadsheet, often in email.

## 2.5 ANSWERS TO CHECK YOUR PROGRESS

1. Cyber stalking
2. Child pornography
3. Software piracy
4. Vishing (voice phishing)

5. White hat
6. Blue hat
7. Cyber Squatting
8. Denial of service attack
9. Macro

## ***2.6 MODEL QUESTIONS***

1. Explain different types of cyber crimes.
2. What is cyber stalking?
3. What is phishing?
4. What is hacking? Classify different types of hackers.
5. What is spamming? Define the criteria based on which an email can be classified as spam.
6. What is computer virus? Define various type of virus.
7. What is cross site scripting?
8. What is data diddling? Explain with an example.

## UNIT III: ORGANIZED CYBER CRIME

### 3.1 LEARNING OBJECTIVES

After going through this unit, you will be able to:

- Understand organized crime
- Categorize different types of organized crime groups
- Know the basic features of organized crime group
- Classify cyber crimes
- Compare cyber crime with cyber terrorism
- Know Information warfare and surveillance
- Understand IT ACT 2000
- Know the applicability of IT Act 2000
- Know the exceptions of IT Act 2000
- Know the basic characteristics of IT Act 2000
- Understand the objectives of IT Act 2000
- Define data privacy
- Know the punishment for cyber crimes defined in IT Act 2000

### 3.2 ORGANIZED CRIME

Organized crime<sup>55</sup> can be defined as serious crime planned, coordinated and conducted by people working together on a continuing basis. Their motivation is often, but not always, financial gain. Organized criminals working together for a particular criminal activity or activities are called an organized crime group. Organized crime group structures vary. Successful organized crime groups often consist of a durable core of key individuals. Around them is a cluster of subordinates, specialists, and other more transient members, plus an extended network of associates. Many groups are often loose networks of criminals that come together for a specific criminal activity, acting in different roles depending on their skills and expertise. Collaboration is reinforced by shared experiences (such as prison), or recommendation from trusted individuals. Others are bonded by family or ethnic ties – some ‘crime families’ are precisely that. Cyber crimes have turned out to be a low-investment, low-risk business with huge returns. Now-a-days these structured crimes are performed are highly organized. There is a perfect hierarchical organizational setup like formal organizations and some of them have reached a level in technical capabilities at par with those of developed nation. They are targeting large financial organizations, defence and nuclear establishments and they are also into online drugs trading.

---

<sup>55</sup> Adopted from: <http://www.nationalcrimeagency.gov.uk/crime-threats/organised-crime-groups>

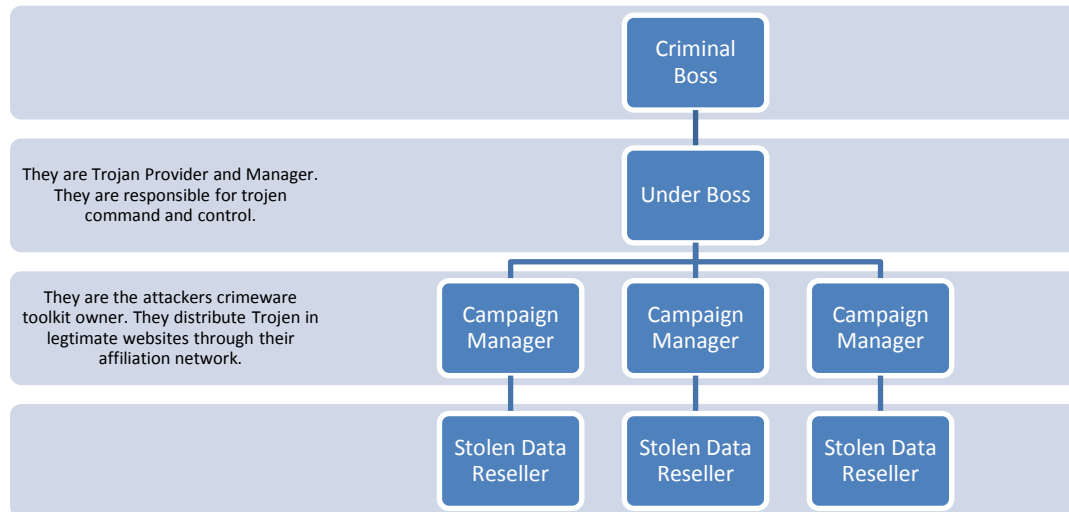


Figure 36: Hierarchical Organizational Structure

The role of all the people in the hierarchy remain changing and it is based on the opportunity. If a hacker who have hacked sensitive data from an organization may use it for financially exploiting the organisation himself. In case, the hacker himself has the technical expertise for it, he will do it himself, otherwise he may find a buyer who is interested in that data and have the technical expertise.

There are some cyber criminals offers on-demand and service. The person, organization or a country may contact these cyber criminals for hacking an organization to gain access to some sensitive data, or create massive denial-of –service attack on their competitors. Based on the demand of the customer the hackers write malware, virus, etc to suit their requirements. An organization effected by a cyber attack, not only faces financial loss, but its reputation is also adversely affected, and the competition organization will defiantly benefited by it.

### 3.2.1 Types of organized crime groups

Three types of organized crime groups have been identified as operating in cyber space:

- traditional organized crime groups that use information and communications technology to enhance their regular criminal activities
- organized cyber criminal groups that operate exclusively online
- organized crime groups made up of ideologically and politically motivated individuals who use information and communications technology to facilitate their criminal conduct.

At minimum, most definitions of an organized crime group include some basic features<sup>56</sup>:

- more than one person involved;
- some semblance of structure;
- a level of continuous operation beyond a one shot deal or job;
- an element of profit motivation.

<sup>56</sup> <https://industryofanonymity.com/category/organised-crime-and-cybercrime/>

### 3.2.2 Classification of Cyber Crimes

Broadly, cybercrime can be classified into following two categories<sup>57</sup>:

- i) Acts wherein a computer or a gadget is used as a tool for an unlawful act. These include cyber defamation, cyber terrorism, cyber-stalking, financial claims, cyber pornography, online ambling, intellectual property crimes, email spoofing, spamming and forgery, and,
- ii) Acts wherein a computer or computer network or a gadget is the target of an unlawful act. These include denial of service, virus/worm, logic bombs, Trojan horse, internet time theft, physically damaging a computer system, theft of information, unauthorized access to computer system or network, e-mail bombing and data diddling.

### 3.2.3 Cyber Crime and Cyber Terrorism

Cyber criminals perform various acts like cyber stalking, on-line harassment, on-line defamation, hacking, and so forth collectively we call it cybercrime<sup>58</sup>. When these activities are managed by organized group systematically and deliberately we term it as CYBER TERRORISM. Cyber terrorism is a well-planned and organized use of technologies by cyber experts resides inside and outside the country for anti-national activities. We can divide these activities as follows:

- 1 Crime against a Person- These types of crimes are targeted towards a person.
- 2 Crime against a Nation- These types of crimes are targeted towards a Nations or groups of nations following same ideology.

### 3.2.4 Information Warfare and surveillance

The term Information warfare<sup>59</sup> refers to the use of information, and attacks on information, as a tool of warfare. Information warfare is comprised of giving the enemy propaganda to convince them to give up and denying them information that might lead to their resistance. It is any action to deny, exploit, corrupt, or destroy the enemy's information and its functions; protecting ourselves against those actions; and exploiting our own military information functions. Information Warfare in its broadest sense is a struggle over the information and communications process, a struggle that began with the advent of human communication and conflict<sup>60</sup>. Over the past few decades, the rapid rise in information and communication technologies and their increasing prevalence in our society has revolutionized the communications process and with it the significance and implications of information warfare. Information warfare is the application of destructive force on a large scale against information assets and systems, against the computers and networks that support the four critical infrastructures (the power grid, communications, financial, and transportation). However, protecting against computer intrusion even on a smaller scale is in the national security interests of the country and is important in the current discussion about information warfare.

<sup>57</sup> Adopted from: <http://works.bepress.com/banday/12/>

<sup>58</sup> Adopted from: <http://giapjournals.com/index.php/hssr/article/view/hssr214/29>

<sup>59</sup> Adopted from: <http://www.iwar.org.uk/iwar/resources/wikipedia/information-warfare.htm>

<sup>60</sup> <http://fas.org/irp/eprint/snyder/infowarfare.htm>



Surveillance<sup>61</sup> is the monitoring of the behavior, activities, or other changing information, usually of people for the purpose of influencing, managing, directing, or protecting them. This can include observation from a distance by means of electronic equipment (such as CCTV cameras), or interception of electronically transmitted information (such as Internet traffic or phone calls); and it can include simple, relatively no- or low-technology methods such as human intelligence agents and postal interception. Surveillance is used by governments for intelligence gathering, the prevention of crime, the protection of a process, person, group or object, or for the investigation of crime. It is also used by criminal organizations to plan and commit crimes such as robbery and kidnapping, by businesses to gather intelligence, and by private investigators. Surveillance is often a violation of privacy, and is opposed by various civil liberties groups and activists. Liberal democracies have laws which restrict domestic government and private use of surveillance, usually limiting it to circumstances where public safety is at risk.

### **3.3 IT ACT 2002<sup>62</sup>**

The Information Technology Act 2000 came into force on 17th Oct., 2000. It consists of 13 Chapters divided into 94 sections. The Act has four schedules on consequential amendments in respect of certain other Acts. Chapters I to VIII are mostly Digital signature related. Chapters IX to XIII are regarding penalties, offences, etc. Information technology (IT), “as defined by the Information Technology Association of America (ITAA), is "the study, design, development, implementation, support or management of computer-based information systems, particularly software applications and computer hardware." IT deals with the use of electronic computers and computer software to convert, store, protect, process, transmit, and securely retrieve information”.

#### **3.3.1 Objects and Reasons**

The Information Technology Act, 2000 provides legal recognition for transactions carried out electronically or by other means as an alternative to paper-based transactions. The need for designing the Information Technology Act, 2000 was to give boost to e-transactions, e-commerce and similar activities associated with commerce and trade and to facilitate e-governance thus making a trouble free interaction of between citizens and government offices. The inspiration for the ACT was a Model Law about electronic commerce adopted by the United Nations Commission on International Trade Law (UNCITRAL) in 1996. The ACT was passed in the year 2000 as Information Technology ACT, 2000.

The Information Technology Act, 2000 has introduced for the first time in India, a range of e-commerce and Internet related criminal offences, and executive powers that will significantly impair the rights of privacy and free speech of both citizens of India and of other countries.

---

<sup>61</sup> <https://en.wikipedia.org/wiki/Surveillance>

<sup>62</sup> This section is adopted from: <http://vle.du.ac.in/mod/book/view.php?id=9573&chapterid=15063>

E-Commerce refers to the trading of goods over the internet. It refers to the business transacted electronically. It is an online buying and selling of products and services for value using Internet Technologies such as e-mail, www, web browsing, etc. The IT Act has been designed to give boost to electronic commerce, e-transactions and also to facilitate e-Governance by means of electronic records.

For commercial transactions, signed and written documents were traditionally used as an evidence as also required by an Indian law. Authentication of the document and at the same time to identify and bind the person who signs the document is the major requirement. In today's world, where everything is communicated online and also all the contracts are completed through electronic communication process, it is important to sign them also digitally for the purpose of authentication and so is the need for cyber laws has arisen.

### **3.3.2 Applicability of the Act**

The Act extends to the whole of India (including Jammu and Kashmir). It applies also to any offence or contravention committed outside India by any person, irrespective of his nationality, if the act or conduct constituting the offence or contravention involves a computer, computer system or computer network located in India.

### **3.3.3 Exceptions to the Act**

Exceptions [Sec 1(14)] “the provisions of the IT Act shall not apply to the following documents:

- “Negotiable Instruments” under the Negotiable Instruments Act, 1881.
- “Power of Attorney” under the Powers of Attorney Act, 1882.
- “Trusts” define in section 3 of the Indian Trusts Act, 1882.
- “Will” define in clause ( h) of Sec( 2) of the Indian Succession Act, 1925 including any other testamentary dispositions;
- Entering into a contract for sale or conveyance of immovable property or any interest in such property.
- Any such class or document which Central Government may notify”.

### **3.3.4 Basic Characteristics of the Act**

The basic characteristics of the ACT are stated as follows:

- 1 Extends to the whole of India.
- 2 Validating all electronic communication contracts legally.
- 3 Digital signatures legal recognition and security procedures for them is provided for.
- 4 Use of cryptography for digital signatures.
- 5 Controller of Certifying Authorities appointment for the grant of license, for certifying keys, for maintaining repositories of digital signatures and regulating the Certifying Authorities.
- 6 Computer related crimes are mentioned in the ACT and accordingly penalties are defined.
- 7 Appointment of Adjudicating Officer

- 8 Establishment of Cyber Regulatory Appellate Tribunal under the Act.
- 9 ACT for offences or contraventions committed outside India.
- 10 No liability of Network service providers in certain cases.
- 11 Police officers right to inspect and search
- 12 Advisory Committee to advise the Central Government and the Controller.

### 3.3.5 Objectives of the Act

The Information Technology (IT) Act, 2000, provides a framework to promote electronic communications in secured environment legally. Information stored in electronic form has many advantages. It is cheaper, creates paper free environment, easier to store and retrieve. But due to lack of appropriate legal framework and security of transactions, users are reluctant to conduct business online. IT Act provides for a regulatory regime to facilitate reliable e-commerce and e-governance. The basic objectives of the IT Act are stated as under:

- 1 Legal recognition of Electronic records.
- 2 Legal recognition of digital signatures.
- 3 Secured electronic communication
- 4 Accessing and retrieving records electronically
- 5 Submission of contracts and records electronically
- 6 Use of authentication in case of digital signatures
- 7 Message integrity by maintaining all standards uniformly
- 8 Use of electronic means for acceptance of contracts and their publication in official gazette
- 9 To prevent all types of crimes related to electronic records such as fraud, forgery etc
- 10 Briefly stated, the IT Act mainly contains provisions to e-commerce, e-governance, and electronic record and digital signature.

### 3.3.6 Definitions

Some important definitions are given below for understanding the concepts and legislative intents. These are:

- **Access** means “with its grammatical variations and cognate expressions means gaining entry into, instructing or communicating with the logical, arithmetical, or memory function resources of a computer, computer system or computer network”;
- **Addressee** means a person who is intended by the originator to receive the electronic record but does not include any intermediary”;
- **Adjudicating officer** “means an adjudicating officer appointed under subsection (1) of section 46;”
- **Affixing digital signature** “means with its grammatical variations and cognate expressions means adoption of any methodology or procedure by a person for the purpose of authenticating an electronic record by means of digital signature”;
- **Appropriate Government** means as respects any matter,- “Enumerated in List II of the Seventh Schedule to the Constitution, Relating to any State law enacted under List III of the Seventh Schedule to the Constitution, the State Government and in any other case, the Central Government”;

- **Asymmetric crypto system** “means a system of a secure key pair consisting of a private key for creating a digital signature and a public key to verify the digital signature”;
- **Certifying Authority** “means a person who has been granted a license to issue a Digital Signature Certificate under section 24”;
- **Certification practice statement** “means a statement issued by a Certifying Authority to specify the practices that the Certifying Authority employs in issuing Digital Signature Certificates”;
- **Computer** “means any electronic magnetic, optical or other high-speed data processing device or system which performs logical, arithmetic, and memory functions by manipulations of electronic, magnetic or optical impulses, and includes all input, output, processing, storage, computer software, or communication facilities which are connected or related to the computer in a computer system or computer network”;
- **Computer network** means the interconnection of one or more computers through— “
  - i. the use of satellite, microwave, terrestrial line or other communication media; and
  - ii. terminals or a complex consisting of two or more interconnected computers whether or not the interconnection is continuously maintained”;
- **Computer resource** “means computer, computer system, computer network, data, computer data base or software”;
- **Computer system** “means a device or collection of devices, including input and output support devices and excluding calculators which are not programmable and capable of being used in conjunction with external files, which contain computer programs, electronic instructions, input data and output data, that performs logic, arithmetic, data storage and retrieval, communication control and other functions”;
- **Controller** “means the Controller of Certifying Authorities appointed under sub- section (1) of section 17”;
- **Cyber Appellate Tribunal** “means the Cyber Regulations Appellate Tribunal established under sub-section (1) of section 48”;
- **Data** “means a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalized manner, and is intended to be processed, is being processed or has been processed in a computer system or computer network, and may be in any form (including computer printouts magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer”;
- **"Digital signature"** means authentication of any electronic record by a subscriber by means of an electronic method or procedure in accordance with the provisions of the section.
- **Digital Signature Certificate** means a Digital Signature Certificate issued under sub-section (4) of section 35”; “
- **Electronic form** “with reference to information means any information generated, sent, received or stored in media, magnetic, optical, computer memory, micro film, computer generated micro fiche or similar device”;
- **Electronic Gazette** means the Official Gazette published in the electronic form”;
- **Electronic record** “means data, record or data generated, image or sound stored, received or sent in an electronic form or micro film or computer generated micro fiche”;

- **Function**, “in relation to a computer, includes logic, control arithmetical process, deletion, storage and retrieval and communication or telecommunication from or within a computer”;
- **Information** “includes data, text, images, sound, voice, codes, computer program, software and databases or micro film or computer generated micro fiche”;
- **Intermediary** “with respect to any particular electronic message means any person who on behalf of another person receives stores or transmits that message or provides any service with respect to that message”;
- **Key pair**, “in an asymmetric crypto system, means a private key and its mathematically related public key, which are so related that the public key can verify a digital signature created by the private key”;
- **Law** “includes any Act of Parliament or of a State Legislature, Ordinances promulgated by the President or a Governor, as the case may be. Regulations made by the President under article 240, Bills enacted as President's Act under sub-clause (a) of clause (1) of article 357 of the Constitution and includes rules, regulations, bye-laws and orders issued or made there under”;
- **License** “means a license granted to a Certifying Authority under section 24”;
- **Originator** “means a person who sends, generates, stores or transmits any electronic message or causes any electronic message to be sent, generated, stored or transmitted to any other person but does not include an intermediary”;
- **Prescribed** “means prescribed by rules made under this Act”;
- **Private Key** “means the key of a key pair used to create a digital signature”;
- **Public key** “means the key of a key pair used to verify a digital signature and listed in the Digital Signature Certificate”;
- **Secure system** “means computer hardware, software, and procedure that- Are reasonably secure from unauthorized access and misuse; Provide a reasonable level of reliability and correct operation; Are reasonably suited to performing the intended functions; and Adhere to generally accepted security procedures”;
  - **Verify** “in relation to a digital signature, electronic record or public key, with its grammatical variations and cognate expressions means to determine whether- the initial electronic record was affixed with the digital signature by the use of private key corresponding to the public key of the subscriber; the initial electronic record is retained intact or has been altered since such electronic record was so affixed with the digital signature”.
- **Security procedure** “means the security procedure prescribed under section 16 by the Central Government”;
- **Subscriber** “means a person in whose name the Digital Signature Certificate is issued”;

### 3.3.7 Why was IT Act 2000 amended in 2008?<sup>63</sup>

1. The main intent to pass the 2000’s Act was to provide legal recognitions to transactions carried out by means of electronic data interchange and other means of electronic communications, commonly known as electronic commerce, which involved the use of

---

<sup>63</sup> Adopted from: <http://mrunal.org/2012/07/yearbook-it-act.html>

alternatives to paper based methods of communication and storage of information and to facilitate the filing of documents of government agencies.

2. But Cyber crime was not looked upon in this act. Even after passing the Act, there was still need to address the specific cyber crimes that were taking place along with the technological advancement.
3. Since the Booming growth of BPO industry and increasing dependence on computers and networks, the incidents of leaking of private data from the BPO's, Banks, Healthcare sectors, telecommunication industry gave rise to provide for a strict legislation to protect the data privacy of all the customers and corporations.
4. Also, the crimes related to privacy breach were rising but as there was no legal framework, specific to the incidents, the IT ACT 2000 seemed ineffective.
5. With the developing demands, the amendments in the IT ACT 2000 were made and IT ACT 2008(amendment) was passed finally on 23rd December 2008.

### **3.3.8 Data privacy**

As per the stated Act, in Section 43A of the amended act, stats as follows:

“43A. Where a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation to the person so affected.

### **3.3.9 What are the responsibilities of a company handling personal data?**

Now, we try to understand the procedures and practices needed to safeguard the sensitive personal data from being stolen, modified without consent of owner, misused or sold in underground markets. Let's make it simple to understand this rule. Say for eg.

1. We have a bank, and as we all know, it deals with sensitive personal data of its customers in its computer networks/servers. Our names, account numbers, passwords, Date of birth, Sex, credit/Debit card details, etc.
2. Therefore, to make sure the bank complies with Mandate of IT ACT, it needs to either get certify with ISO 27001 (world renowned standard for data protection) or it may develop its own security manual which describes full in-depth details of its IT assets, the Life cycle of assets, the physical security measures(viz. CCTVs, Locks, vaults, fire prevention/detection, temperature controls in server rooms, security guard details and so on).
3. It should also have a detailed Business Continuity plan (In case of any natural/manmade calamity the organization must have a detailed backup process so as to continue its business),
4. Other applicable procedures of separation of duties of key personals, background checks of employees before employing, etc.
5. Not only Banks, but the BPOs/KPOs, hospitals, and various other businesses which deals with sensitive personal data, need to comply with this act.

### 3.3.10 What is the punishment for cyber crimes?

<b>SECTION OF THE ACT</b>	<b>OFFENCE</b>	<b>PENALTY</b>
Section 65	Tampering with computer source documents.	Imprisonment up to 3 years or a fine of 2 lakh rupees, or both.
Section 66	Hacking & Breach of confidentiality of personal information as per sec.43 & 43A	Imprisonment up to 3 years or a fine up to 5 lakh rupees or both. (For Hacking, fine is 2 lakh rupees, imprisonment is 3 years)
Section 66A	Sending offensive messages through communication service, etc.	Imprisonment of 3 years & fine.
Section 66B	Dishonestly receiving stolen resource or communication device.	Imprisonment of 3 years & fine.
Section 66C & D	Identity theft	Imprisonment up to 3 years & fine up to 1 lakh rupees.
Section 66E	Violation of personal Privacy	Imprisonment up to 3 years or fine not exceeding 2 lakh rupees or with both.
Section 66F	Cyber terrorism	Imprisonment for life.
Section 67, 67A & B	Publishing or transmitting obscene material in electronic form./pornography/child pornography	Imprisonment term up to 5/7 years and fine up to 10 lakh rupees.
Section 67C	Failure to preserve and retain information by intermediaries	Imprisonment for 3 years and fine.

### 3.3.11 Who can conduct RAIDS AND INVESTIGATION for Cybercrimes?

- As per the act, previously, a police officer not less than a rank of DySP can investigate or conduct a raid at a public place without a warrant, but as per the amendment, the rank of Police Inspector can investigate the offences and conduct raids. (Section 78-amended)
- Also, As per the provisions in the act, and according to section 46(amended), adjudicating officer shall exercise jurisdiction to adjudicate matters in which claim for injury or damage does not exceed 5 crore. If this claim exceeds above 5 crore, then the matter is looked upon by the competent court.

For further details on IT ACT 2000, the learners are encouraged to visit:  
<http://www.dot.gov.in/act-rules/information-technology-act-2000>

## 3.4 SUMMARY

1. Organized crime can be defined as serious crime planned, coordinated and conducted by people working together on a continuing basis.
2. Collaboration is reinforced by shared experiences (such as prison), or recommendation from trusted individuals.
3. Many groups are often loose networks of criminals that come together for a specific criminal activity, acting in different roles depending on their skills and expertise.
4. There is a perfect hierarchical organizational setup like formal organizations and some of them have reached a level in technical capabilities at par with those of developed nation.
5. There are some cyber criminals offers on-demand and service.
6. Information warfare is comprised of giving the enemy propaganda to convince them to give up and denying them information that might lead to their resistance.
7. The Information Technology Act 2000 came into force on 17th Oct., 2000.
8. The Information Technology Act, 2000 provides legal recognition for transactions carried out electronically or by other means as an alternative to paper-based transactions.
9. **Access** means “with its grammatical variations and cognate expressions means gaining entry into, instructing or communicating with the logical, arithmetical, or memory function resources of a computer, computer system or computer network”;
10. **Data** means a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalized manner, and is intended to be processed, is being processed or has been processed in a computer system or computer network, and may be in any form (including computer printouts magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer.

## 3.5 CHECK YOUR PROGRESS

1. When these activities are managed by organized group systematically and deliberately we term it as \_\_\_\_\_ .



2. The term \_\_\_\_\_ refers to the use of information, and attacks on information, as a tool of warfare.
3. \_\_\_\_\_ is the monitoring of the behavior, activities, or other changing information, usually of people for the purpose of influencing, managing, directing, or protecting them.
4. IT ACT 2000 consists of 13 Chapters divided into \_\_\_\_ sections.
5. Chapters I to VIII are mostly \_\_\_\_\_ related.
6. \_\_\_\_\_ refers to the trading of goods over the internet.
7. \_\_\_\_\_ of the document and at the same time to identify and bind the person who signs the document is the major requirement.
8. \_\_\_\_\_ means the key of a key pair used to verify a digital signature and listed in the Digital Signature Certificate.

### **3.6 ANSWERS TO CHECK YOUR PROGRESS**

- 1 Cyber Terrorism
- 2 Information warfare
- 3 Surveillance
- 4 94
- 5 Digital signature
- 6 E-Commerce
- 7 Authentication
- 8 Public key

### **3.7 MODEL QUESTIONS**

1. What is an organized cyber crime.?Explain.
2. Explain different types of organized crime groups. What are the basic features of an organized crime group.
3. What is Information warfare?
4. What is cyber terrorism?
5. What are the exceptions in the IT Act 2000?
6. List the basic characteristics of IT Act 2000.
7. What are the objectives of IT Act 2000?
8. What is certifying authority?
9. Define digital signature.
10. Why was IT Act 2000 amended in 2008?
11. What s data privacy? What are the responsibilities of a company handling personal data?
12. Who can conduct RAIDS AND INVESTIGATION for Cybercrimes?

## UNIT IV: CYBER CRIMES - CASE STUDIES

### 4.1 LEARNING OBJECTIVES

After going through this unit, you will be able to:

- Know the different type of cyber crimes.
- Know various cases related to cyber crimes.
- Understand methodology of cyber criminals.
- Understand the safety measures to various cyber crimes.

### 4.2 INTRODUCTION

From business, industry, government to not-for-profit organizations, the internet has simplified business processes such as sorting, summarizing, coding, editing, customized and generic report generation in a real-time processing mode. However, it has also brought unintended consequences such as criminal activities, spamming, credit card frauds, ATM frauds, phishing, identity theft and a blossoming haven for cybercriminal miscreants to perpetrate their insidious acts. Over the past twenty years, immoral cyberspace users have continued to use the internet to commit crimes<sup>64</sup>. This unit aims to introduce the learner with various types of cyber crimes along with the case studies so that they have fair idea about different types the cyber crimes. It will be followed by discussion on some of the prevention measures for the users.

### 4.3 CYBER CRIME - CASE STUDIES

#### 4.3.1 Cyber Stalking

This is one of the most popular about internet crime in the modern world Cyber stalking can be defined as the repeated acts of harassment or threatening behavior of the cyber criminal towards the victim by using the internet services. Online harassment can be divided into direct and indirect harassment. *Direct* harassment includes the use of pagers, cell phones and the email to send messages of hate, obscenities and threats, to intimidate a victim. e.g., the majority of offline stalkers will attempt to contact their victim, and most contact is restricted to mail and/or telephone communications. On the other hand *indirect* harassment includes the use of the Internet to display messages of hate, threats or used to spread false rumors about a victim. Messages can be posted on web pages, within chat groups or bulletin boards. This form of harassment is the electronic equivalent of placing pinups on a factory wall, and if the display of such material from the victim's perspective causes offence it will amount to harassment.

Stalking in the internet happens when the perpetrator follows the victim continuously by leaving unwanted messages. The motivation of stalkers may be from the following four reasons:

- (i) sexual harassment

---

<sup>64</sup> <http://www.ijcrsee.com/index.php/ijcrsee/article/view/11/114>

- (ii) obsession for love
- (iii) revenge and hate
- (iv) ego and power trips.

The stalker disturbs their targets through private emails as well as public message. Most of the cases are reported where the target of cyber stalking are women especially of the age group of 16 to 35. Stalking and harassment are distinctive in law since the offending behavior is said to occur only when the victim reports him/her self to be distressed as a result of the behavior of another to whom they believe to be threatening. The victim's perception of the offending behavior and its effects are therefore pivotal in providing criteria on which to make a charge.

#### **4.3.1.1 Cyberstalking Facts**

- Over 20,000 cases of cyberstalking are being reported each year.
- Over 90% of victims are women.
- It is estimated there may be as many as 500,000 online victims each year.
- Cyberstalkers feel they are anonymous and can get away with anything.
- When caught, most cyberstalkers say they didn't mean to do it, or for it to go so far.
- Most instances are not related to romances gone sour; a majority of the cases are stranger-to-stranger.

#### **4.3.1.2 Examples of Cyberstalking**

Some of the common examples of the cyberstalking are:

- Threatening or harassing email.
- Flaming - online verbal abuse.
- Mass unsolicited email.
- Identity theft.
- Leaving improper messages at guestbook's or newsgroups from the victim.
- Initiating directed computer viruses.
- Email forgery - sending false or damaging email from the victim - usually to people they know like co-workers, employees, neighbors, etc.

#### **4.3.1.3 Guidelines for victim of Cyberstacking**

If you have become a victim of cyberstalking, below are the guidelines to be followed:

- Where the offender is known, send the stalker a written message indicating that any further contact is unwanted.
- Victims should not communicate with the stalker after the warning message.
- If harassment continues, the victim should contact the stalker's Internet service provider, as well as their own. Service providers often have services to block and filter unwanted communications.
- Collect all evidence including e-mails, postings, or other communications in hardcopy or in an electronic form.
- Contact local law enforcement agencies to see what action can be taken.

- Consult your local computer store about encryption and privacy protection software.
- Consider changing your e-mail address, Internet service provider and home telephone number.
- Contact online directories to remove yourself from their listings.
- Never agree to meet with a cyber stalker to work things out face-to-face.
- Never leave your computer logged-in unattended.
- Choose a good account password and change it frequently, the best passwords don't spell anything and don't follow a logical pattern.
- Make your password 7 letters long because the longer the password the harder it will be to break (there are more 7 letter words in the English language than 6 or 8 letter words).
- Review your e-mail signature and headers; do not reveal any personal information about yourself.
- Contact the Local Law enforcement agencies; they fight crime on the Internet.
- Tell family, friends and co-workers about the harassment so that they can provide support.

#### **4.3.1.4 Prevention Tips from Cyberstalking**

Below are some tips useful for the prevention of cyber stalking:

- Do not share personal information (real name, address, phone number, school information, marital status, occupation, income or passwords) in public spaces anywhere online, nor give it to strangers, including in email or chat rooms. Do not use your real name or nickname as your screen name or user ID. Pick a name that is gender-and-age neutral. And do not post personal information as part of any user profiles.
- Some filtering software programs can prevent children from posting or emailing an address, telephone number, or credit card number.
- Be extremely cautious about meeting online acquaintances in person. If you choose to meet, do so in a public place and take along a friend.
- Make sure your ISP and Internet Relay Chat (IRC) network have an acceptable use policy that prohibits cyberstalking. If your network fails to respond to your complaints, consider switching to a provider that is more responsive to user complaints.
- If a situation online becomes hostile, log off or surf elsewhere. If a situation places you in fear, contact a local law enforcement agency.

#### **4.3.1.5 Case Study on Cyber stalking**

*Case 1: Cyber stalking Case Involving Violent Threats against Art Dealers and Their Children Leads to Five-Year Federal Prison Term.*

Jason White, The owner of a Temecula art gallery in Los Angeles , who stalked, harassed and attempted to extort as much as \$300,000 from art world professionals was sentenced to 60 months in federal prison. He was pleaded guilty in March 2014 to two counts of federal stalking, was sentenced today by United States District Judge Stephen V. Wilson.

White targeted his former employer, an art publisher, as well as White's supervisor at the art publisher's company. After creating derogatory websites in the art publisher's name, White allegedly sent threatening text messages to the art publisher, the publisher's son, and his former supervisor. In a text message to his former supervisor, he threatened to find her family and make her pay with "fear, anguish and pain." On several occasions, White obtained pictures of her child and sent pictures of the child to the victim with comments such as "it will be very unfortunate if something was to happen to him." White's "conduct also demonstrates a disturbing and escalating pattern of stalking conduct, particularly since he committed these crimes less than one year after a restraining order was filed against him by another former employer for identical cyber stalking and extortion conduct," according to the government's sentencing position papers. "As defendant intended, his stalking crimes traumatized his victims." Victims felt terrorized by the barrage of threatening e-mails and texts that White sent them.

White was arrested by the FBI on February 12 after engaging in a six-month stalking and extortion scheme that targeted art world professionals with whom he had had business relationships. When those business relationships ended, White posted derogatory information about his former associates on websites he had created, and then used threatening e-mails to demand hundreds of thousands of dollars in exchange for taking the websites down. White repeatedly made extortionate demands through harassing text messages and e-mails, and when his demands were not met, he threatened violence against the victim families, including their children. Given the ominous, angry and relentless nature of the messages, the victims had a reasonable fear that defendant planned to hunt down and kill their spouses and children.

**Case II:** *First reported cyberstalking case of India- Ritu Kohli Vs. Manish Kathuria.*

In one of the first cases of cyberstalking in India in 2000<sup>65</sup>, Delhi police booked Manish Kathuria for "intending to insult the modesty of a woman". Kathuria pretended to be Ritu Kohli, the wife of his former colleague, in internet chat rooms, made her phone number public and solicited sex. Though police tracked him down, the lack of specific laws meant he got off lightly.

### **4.3.2 erawmosnaR**

Ransomware is a type of malware that prevents or limits users from accessing their system. This type of malware forces its victims to pay the ransom through certain online payment methods in order to grant access to their systems, or to get their data back. Some ransomware encrypts files (called Cryptolocker). Ransomware spreads through e-mail attachments, infected programs and compromised websites. A ransomware malware program may also be called a cryptovirus, cryptotrojan or cryptoworm. Attackers may use one of several different approaches to extort money from their victims. After a victim discovers he cannot open a file, he receives an email ransom note demanding a relatively small amount of money in exchange for a private key. The attacker warns that if the ransom is not paid by a certain date, the private key will be destroyed and the data will be lost forever.

---

<sup>65</sup> <http://epaper.timesofindia.com/Repository/ml.asp?Ref=VE9JQ0gvMjAxMy8wMy8xOCNBcjAwNDAY>

The victim is duped into believing he is the subject of a police inquiry. After being informed that unlicensed software or illegal web content has been found on his computer, the victim is given instructions for how to pay an electronic fine.

The malware surreptitiously encrypts the victim's data but does nothing else. In this approach, the data kidnapper anticipates that the victim will look on the Internet for how to fix the problem and makes money by selling anti-ransomware software on legitimate websites. To protect against data kidnapping, experts urge that users backup data on a regular basis. If an attack occurs, do not pay a ransom. Instead, wipe the disk drive clean and restore data from the backup. The members of cryptolocker family are:

1. Dirty Decrypt
2. CryptoLocker
3. CryptoWall / Cryptodefense
4. Critroni / CTB Locker
5. TorrentLocker
6. Cryptographic Locker

#### 4.3.2.1 How does Cryptolocker work?

After infecting the victim's computer, CryptoLocker generates a Unique ID and sends it to a server controlled by the attackers. The server then generates a public-private key pair (based on the received Unique ID) and sends the public key back to computer. The CryptoLocker malware, running on victim's computer uses this public key to encrypt different type of files (documents, spread sheets but also pictures as well as Internet Security Certificate files) found on the victim's machine. The virus will search for files to encrypt on all locations and drives it can access from the victim's computer, including network drives and resources on other computers or servers.

#### 4.3.2.2 Prevention Tips from RANSOMWARE

1. **Back up your data:** The single biggest thing that will defeat ransomware is having a regularly updated backup. If you are attacked with ransomware you may lose that document you started earlier this morning, but if you can restore your system to an earlier snapshot or clean up your machine and restore your other lost documents from backup, you can rest easy.
2. **Show hidden file-extensions:** One way that Cryptolocker frequently arrives is in a file that is named with the extension “.PDF.EXE”, counting on Window’s default behavior of hiding known file-extensions. If you re-enable the ability to see the full file-extension, it can be easier to spot suspicious files.
3. **Filter EXEs in email:** If your gateway mail scanner has the ability to filter files by extension, you may wish to deny mails sent with “.EXE” files, or to deny mails sent with files that have two file extensions, the last one being executable (“\*. \*.EXE” files, in filter-speak).
4. **Disable files running from AppData/LocalAppData folders:** You can create rules within Windows or with Intrusion Prevention Software, to disallow a particular, notable

behavior used by Cryptolocker, which is to run its executable from the App Data or Local App Data folders.

5. **Use the Cryptolocker Prevention Kit:** The Cryptolocker Prevention Kit is a tool created by Third Tier that automates the process of making a Group Policy to disable files running from the App Data and Local App Data folders, as well as disabling executable files from running from the Temp directory of various unzipping utilities.
6. **Disable RDP:** The Cryptolocker/Filecoder malware often accesses target machines using Remote Desktop Protocol (RDP), a Windows utility that allows others to access your desktop remotely. If you do not require the use of RDP, you can disable RDP to protect your machine from Filecoder and other RDP exploits.
7. **Patch or Update your software:** These next two tips are more general malware-related advice, which applies equally to Cryptolocker as to any malware threat. Malware authors frequently rely on people running outdated software with known vulnerabilities, which they can exploit to silently get onto your system.
8. **Use a reputable security suite:** It is always a good idea to have both anti-malware software and a software firewall to help you identify threats or suspicious behavior. Malware authors frequently send out new variants, to try to avoid detection, so this is why it is important to have both layers of protection.
9. **Disconnect from WiFi or unplug from the network immediately:** If you run a file that you suspect may be ransomware, but you have not yet seen the characteristic ransomware screen, if you act very quickly you might be able to stop communication with the server before it finish encrypting your files.
10. **Use System Restore to get back to a known-clean state:** If you have System Restore enabled on your Windows machine, you might be able to take your system back to a known-clean state. But, again, you have to out-smart the malware. Newer versions of Cryptolocker can have the ability to delete “Shadow” files from System Restore, which means those files will not be there when you try to replace your malware-damaged versions.

#### 4.3.2.3 Case studies on Ransomware

##### *Case I: Ransomware Suspects, Dutch Police Relied on a Russian Security Firm*

In the latest example of the close-knit relationship between private cybersecurity companies and law enforcement, two men from the Netherlands have been arrested on suspicion of creating a piece of ransomware that infuriated victims for just over a year<sup>66</sup>.

The Dutch police, arrested an 18 and a 22 year-old in relation to CoinVault, a moderately successful ransomware campaign. The busts came around not necessarily because of gumshoe detective work, but relied on information provided to police by the Russian company Kaspersky. The CoinVault campaign started in May 2014. After being used to infect computers running

---

<sup>66</sup> <http://motherboard.vice.com/read/kaspersky-helps-police-catch-ransomware-suspects>

various versions of Windows, CoinVault would, in traditional ransomware style, encrypt all of a victim's files until he or she handed over a hefty fine, payable in Bitcoin.

**Case II:** *A police department in Massachusetts has paid \$750 for two bitcoins to release files encrypted by the increasingly pervasive Cryptolocker ransomware*

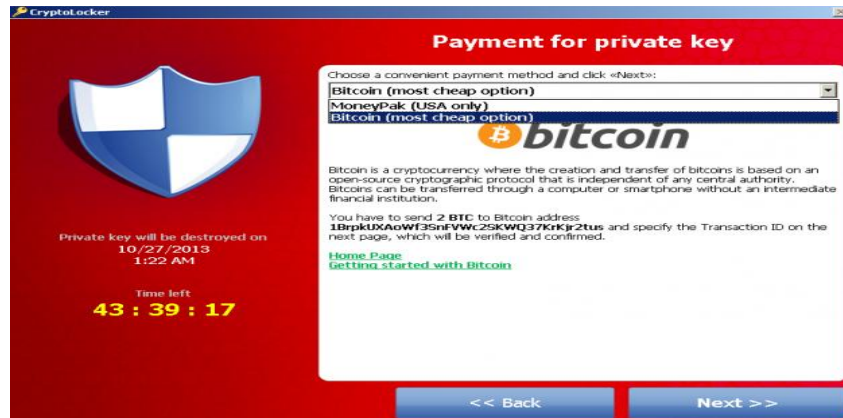


Figure 37: Bitcoin

A computer in the police department of Swansea, Massachusetts was hit by the CryptoLocker ransomware on 6 November 2015. CryptoLocker is a particularly pernicious piece of malware that is typically spread as a malicious attachment in emails which look to come from financial institutions or postal services. The malware infected the computer in the Swansea police department and encrypted files on the PC's hard drive including "images and word documents" which could include police reports and arrest photos of suspects.

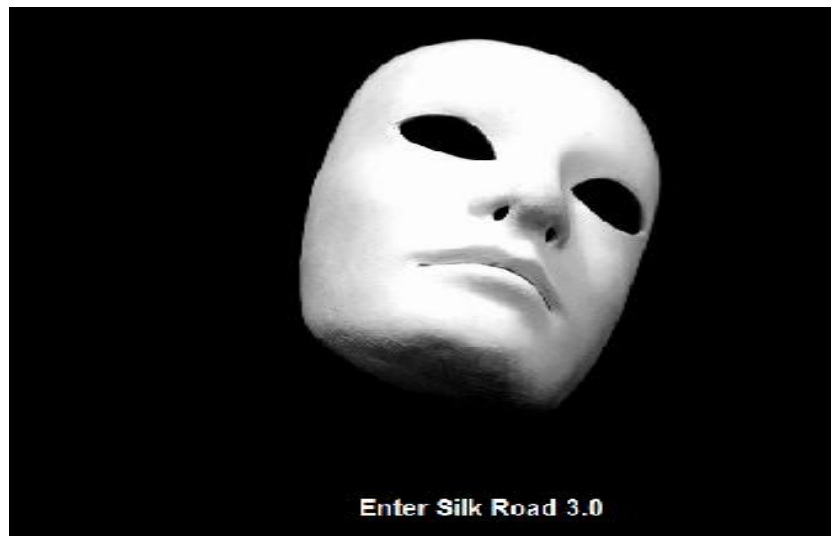
The police department clearly had no backup system in place as it paid the ransom of two bitcoins, despite FBI guidance not to pay the cyber-criminals behind the attack. At the time two bitcoins were worth \$750 but if the police had to pay up, the price would be \$1,300 as bitcoin's value has risen considerably in November 2015.

### 4.3.3 Silkroad

Silkroad, a darknet market infamous for selling illegal drugs that worked in a similar way to eBay but its access was restricted to those who have the special software required to access the site. Some of the categories of drugs sold on Silkroad include stimulants, prescription, ecstasy, cannabis and steroids among many others. Apart from drugs, Silkroad also sold fake driver's licenses. It restricted the sale of various items including child pornography, weapons and child pornography.

Silk Road, an underground marketplace that used bitcoin as currency and which had reportedly facilitated a billion dollars in sales over the two years of its existence. The charges included drug trafficking, computer hacking and money laundering.





*Figure 38: Silkroad*

The online promotion of ‘drug shopping’ and user information networks is of increasing public health and law enforcement concern. An online drug marketplace called ‘Silk Road’ has been operating on the ‘Deep Web’ and was designed to revolutionize contemporary drug consumerism.

A single case study approach explored a ‘Silk Road’ user’s motives for online drug purchasing, experiences of accessing and using the website, drug information sourcing, decision making and purchasing, outcomes and settings for use, and perspectives around security. There is a handy site that acts as a layer between the surface internet and the dark web.

#### **4.3.3.1 Case Studies on Silkroad**

##### **Case : *Two Silk Road Drug Importers Sentenced To Jail***

Two men from South Devon have been sentenced for selling illegal drugs and using the darknet to acquire them. The 2 men are Jamie McAllister and Nathan Wilson. McAllister, 35, claims to be a businessman specializing in making beds while Wilson, 30, is a council worker. Investigations showed that 3,800 pounds had been transferred through Western Union in exchange for 2300g of cannabis and 74.6g of heroin. These drugs have a street value of 14,000 pounds in UK. The packages containing drugs from Silkroad were intercepted by border officials. Silkroad was first formed in 2011, operated as a Tor hidden service and conducted transactions using bitcoins to prevent tracing information of buyers and sellers. The FBI acquired information about the illegal activities taking place in the site and they shut it down in 2013. Ross William Ulbricht was arrested in October 2013 under the charges of being the owner of Silkroad. In May 2015, Ulbricht was sentenced to life imprisonment without any possibility of parole. Despite the shutdown of Silkroad, other darknet markets continue to emerge. In an investigation that was carried out about the darknet markets, it was discovered that not everyone who buys from there wants to do so. Some may need prescription medications which are expensive in local pharmacies hence they turn to darknet markets where they are cheaper.

### 4.3.4 Phishing

Global volumes of victims of phishing emails increased significantly compared with recent years which involve the tremendous increase in the use of online banking, mobile banking and e-commerce, there has been a corresponding growth in the incidents of phishing being used to carry out financial frauds. Phishing involves fraudulently acquiring sensitive information (e.g. passwords, user personal details, credit card details etc) by masquerading as a trusted entity.

A scammer contacts you out of the blue pretending to be from a legitimate business such a bank, telephone or internet service provider<sup>67</sup>. You may be contacted by email, social media, phone call, or text message. The scammer asks you to provide or confirm your personal details. For example, the scammer may say that the bank or organisation is verifying customer records due to a technical error that wiped out customer data. Or, they may ask you to fill out a customer survey and offer a prize for participating.

Alternatively, the scammer may alert you to 'unauthorised' or suspicious activity on your account'. You might be told that a large purchase has been made in a foreign country and asked if you authorised the payment. If you reply that you didn't, the scammer will ask you to confirm your credit card or bank details so the 'bank' can investigate. In some cases the scammer may already have your credit card number and ask you to confirm your identity by quoting the 3 or 4 digit security code printed on the card.

Phishing messages are designed to look genuine, and often copy the format used by the organisation the scammer is pretending to represent, including their branding and logo. They will take you to a fake website that looks like the real deal, but has a slightly different address. For example, if the legitimate site is 'www.realbank.com', the scammer may use an address like 'www.reallbank.co.in'.

If you provide the scammer with your details online or over the phone, they will use them to carry out fraudulent activities, such as using your credit cards and stealing your money.

---

<sup>67</sup> <https://www.scamwatch.gov.au/types-of-scams/attempts-to-gain-your-personal-information/phishing>

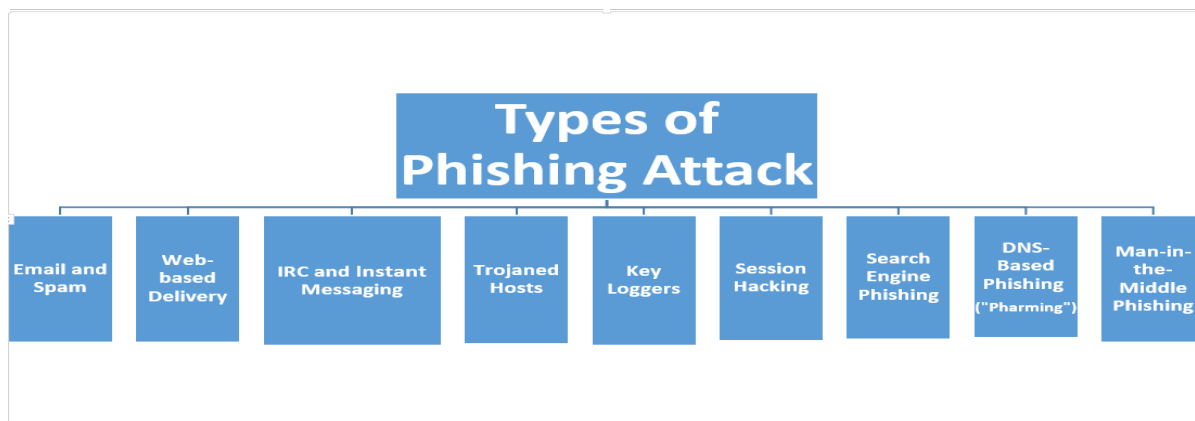


Figure 39: Types of Phishing

Phishing has spread beyond email to include VOIP, SMS, instant messaging, social networking sites, and even multiplayer games.

#### 4.3.4.1 Phishing Types

Below are some major categories of phishing.

1. **Clone Phishing:** In this type phisher creates a cloned email. He does this by getting information such as content and recipient addresses from a legitimate email which was delivered previously, then he sends the same email with links replaced by malicious ones. He also employs address spoofing so that the email appears to be from the original sender. The email can claim to be a re-send of the original or an updated version as a trapping strategy.
2. **Spear Phishing:** Spear phishing targets at a specific group. So instead of casting out thousands of emails randomly, spear phishers target selected groups of people with something in common, for example people from the same organization. Spear phishing is also being used against high-level targets, in a type of attack called “whaling”.
3. **Phone Phishing:** This type of phishing refers to messages that claim to be from a bank asking users to dial a phone number regarding problems with their bank accounts. Traditional phone equipment has dedicated lines, so Voice over IP, being easy to manipulate, becomes a good choice for the phisher. Once the phone number, owned by the phisher and provided by a VoIP service, is dialed, voice prompts tell the caller to enter her account numbers and PIN. Caller ID spoofing, which is not prohibited by law, can be used along with this so that the call appears to be from a trusted source.
4. **Web Spoofing:** A phisher could forge a website that looks similar to a legitimate website, so that victims may think this is the genuine website and enter their passwords and personal information, which is collected by the phisher. Modern web browsers have certain built-in security indicators that can protect users from phishing scams, including domain name highlighting and https indicators. However, they are often neglected by careless users.
5. **Deceptive Phishing:** The term "phishing" originally referred to account theft using instant messaging but the most common broadcast method today is a deceptive email

message. Messages about the need to verify account information, system failure requiring users to re-enter their information, fictitious account charges, undesirable account changes, new free services requiring quick action, and many other scams are broadcast to a wide group of recipients with the hope that the unwary will respond by clicking a link to or signing onto a bogus site where their confidential information can be collected.

6. **Malware-Based Phishing:** Malware-Based Phishing refers to scams that involve running malicious software on users' PCs. Malware can be introduced as an email attachment, as a downloadable file from a web site, or by exploiting known security vulnerabilities--a particular issue for small and medium businesses (SMBs) who are not always able to keep their software applications up to date.
7. **Keyloggers and Screenloggers:** Keyloggers and Screenloggers are particular varieties of malware that track keyboard input and send relevant information to the hacker via the Internet. They can embed themselves into users' browsers as small utility programs known as helper objects that run automatically when the browser is started as well as into system files as device drivers or screen monitors.
8. **Session Hijacking:** Session Hijacking describes an attack where users' activities are monitored until they sign in to a target account or transaction and establish their bona fide credentials. At that point the malicious software takes over and can undertake unauthorized actions, such as transferring funds, without the user's knowledge. Web Trojans pop up invisibly when users are attempting to log in. They collect the user's credentials locally and transmit them to the phisher.
9. **Hosts File Poisoning:** Hosts File Poisoning. When a user types a URL to visit a website it must first be translated into an IP address before it's transmitted over the Internet. The majority of SMB users' PCs running a Microsoft Windows operating system first look up these "host names" in their "hosts" file before undertaking a Domain Name System (DNS) lookup. By "poisoning" the hosts file, hackers have a bogus address transmitted, taking the user unwittingly to a fake "look alike" website where their information can be stolen. System Reconfiguration Attacks modify settings on a user's PC for malicious purposes. For example: URLs in a favourites file might be modified to direct users to look alike websites. For example: a bank website URL may be changed from "bankofabc.com" to "bancofab.com".
10. **Data Theft:** Unsecured PCs often contain subsets of sensitive information stored elsewhere on secured servers. Certainly PCs are used to access such servers and can be more easily compromised. Data theft is a widely used approach to business espionage. By stealing confidential communications, design documents, legal opinions, employee related records, etc., thieves profit from selling to those who may want to embarrass or cause economic damage or to competitors.
11. **DNS-Based Phishing:** DNS-Based Phishing ("Pharming"). Pharming is the term given to hosts file modification or Domain Name System (DNS)-based phishing. With a pharming scheme, hackers tamper with a company's hosts files or domain name system so that

requests for URLs or name service return a bogus address and subsequent communications are directed to a fake site. The result: users are unaware that the website where they are entering confidential information is controlled by hackers and is probably not even in the same country as the legitimate website.

12. **Content-Injection Phishing:** Content-Injection Phishing describes the situation where hackers replace part of the content of a legitimate site with false content designed to mislead or misdirect the user into giving up their confidential information to the hacker. For example, hackers may insert malicious code to log user's credentials or an overlay which can secretly collect information and deliver it to the hacker's phishing server.
13. **Man-in-the-Middle Phishing:** Man-in-the-Middle Phishing is harder to detect than many other forms of phishing. In these attacks hackers position themselves between the user and the legitimate website or system. They record the information being entered but continue to pass it on so that users' transactions are not affected. Later they can sell or use the information or credentials collected when the user is not active on the system.
14. **Search Engine Phishing:** Search Engine Phishing occurs when phishers create websites with attractive (often too attractive) sounding offers and have them indexed legitimately with search engines. Users find the sites in the normal course of searching for products or services and are fooled into giving up their information. For example, scammers have set up false banking sites offering lower credit costs or better interest rates than other banks. Victims who use these sites to save or make more from interest charges are encouraged to transfer existing accounts and deceived into giving up their details.
15. **Fast flux Phishing:** Fast flux is a DNS technique used by botnets to hide phishing and malware delivery sites behind an ever-changing network of compromised hosts acting as proxies.

#### 4.3.4.2 Anti-Phishing Groups

- a. PhishTank, launched in October 2006, is a collaborative clearing house for data and information about phishing on the Internet. PhishTank employs a sophisticated voting system that requires the community to vote “phish” or “not phish”, reducing the possibility of false positives and improving the overall breadth and coverage of the phishing data. It also provides an open API for developers and researchers to integrate anti-phishing data into their applications at no charge. PhishTank is backed by OpenDNS, a public DNS resolver; OpenDNS utilizes PhishTank data to prevent phishing attacks for their users.
- b. Anti-Phishing Working Group (APWG) is an international consortium, formed in 2003, brings together businesses affected by phishing attacks, security products and services companies, law enforcement agencies, government agencies, trade association, regional international treaty organizations, and communications companies

#### 4.3.4.3 Legal Clause

Sections 43 and 66 of Information Technology Act and sections 419, 420 and 468 of Indian Penal Code. All persons involved in creating and sending the fraudulent emails and creating and

maintaining the fake website. The persons who misuse the stolen or “phished” information are also liable. The motive is Illegal financial gain.

Example: The attacker registers a domain name using fictitious details. The domain name is usually such that can be misused for spoofing e.g. XYZ\_Bank.com has its website at www.XYZ\_Bank.com.com The attacker can target XYZ\_Bank.com customers using a domain name like www.XYZ\_Bank.com-bank-customerlogin.com The attacker then sends spoofed emails to the victims. e.g. the emails may appear to come from info@XYZ\_Bank.com The fake website is designed to look exactly like the original website.

#### 4.3.4.4 Case Studies in Phishing

**Case I:** The landmark decision of the Adjudicator of Tamil Nadu in the case of Umashankar Vs ICICI Bank, ordering payment of a compensation of Rs 12.85 lakhs to the victim of a Phishing fraud was covered by a few publications. It appears that the media has been very diffident of covering the landmark case and probably the PR machinery of the Bank has been working overtime to ensure that the case is not publicised.

**Case II:** UTI Bank, a leading private bank promoted by India's largest financial institution, Unit Trust of India (UTI). A URL on Geocities that is almost a facsimile version of the UTI Bank's home page is reported to be circulating amongst email users<sup>68</sup>. The web page not only asks for the account holder's information such as user and transaction login and passwords, it has also beguilingly put up disclaimer and security hazard statements. The tricky link is available on <http://br.geocities>

If any unsuspecting account holder enters his login id, password, transaction id and password in order to change his details as 'advised' by the bank, the same info is sent vide mailform.cz (the phisher's database). After investigation, we found that Mailform is a service of PC Svet, which is a part of the Czech company PES Consulting. The Webmaster of the site is a person named Petr Stastny whose e-mail can be found on the web page. Top officials at UTI Bank said that they have reported the case to the Economic Office Wing, Delhi Police. The bank has also engaged the services of Melbourne-based FraudWatch International, a leading anti-phishing company that offers phishing monitoring and take-down solutions”. As per the findings of UTI Bank's security department, the phishers have sent more than 1,00,000 emails to account holders of UTI Bank as well as other banks.

#### 4.3.5 419(Advance-Fee Fraud) Scam

419 Fraud, after the relevant section of the Criminal Code of Nigeria, these communications are also referred to as Nigerian Letters. They are a form of advance-fee fraud in which a victim is persuaded to pay money upfront for further financial reward which never materializes.

##### 4.3.5.1 What is 419 (Advance-fee Fraud) Scam?

An advance-fee fraud, also known as a 419 fraud, is a type of scam in which the victim is convinced to advance money to a stranger. In all such scams, the victim is led to expect that a

---

<sup>68</sup> <http://www.cyberlawsindia.net/cases1.html>

much larger sum of money will be returned to him or her. The victim, of course, never receives any of this money.

Those who fall for an advance-fee fraud and forward money to the criminal are likely to be targeted for additional payments. That is, the criminal may claim that a second or third advance is necessary before the victim will be entitled to receive the promised money.

**Nigerian Advanced Fee Fraud Email Scams**

Lagos, Nigeria  
Attention: The President/CEO

Dear Sir,

Confidential Business Proposal

Having consulted with my colleagues and based on the information gathered from the Nigerian Chambers Of Commerce And Industry, I have the privilege to request your assistance to transfer the sum of \$47,500,000.00 (forty seven million, five hundred thousand United States dollars) into your accounts. The above sum resulted from an over-invoiced contract, executed, commissioned and paid for about five years (5) ago by a foreign contractor. This action was however intentional and since then the fund has been in a suspense account at The Central Bank Of Nigeria Apex Bank.

We are now ready to transfer the fund overseas and that is where you come in. It is important to inform you that as civil servants, we are forbidden to operate a foreign account; that is why we require your assistance. The total sum will be shared as follows: 70% for us, 25% for you and 5% for local and international expenses incidental to the transfer.

The transfer is risk free on both sides. I am an accountant with the Nigerian National Petroleum Corporation (NNPC). If you find this proposal acceptable, we shall require the following documents:

- (a) your banker's name, telephone, account and fax numbers.
- (b) your private telephone and fax numbers —for confidentiality and easy communication.
- (c) your letter-headed paper stamped and signed.

Alternatively we will furnish you with the text of what to type into your letter-headed paper, along with a breakdown explaining, comprehensively what we require of you. The business will take us thirty (30) working days to accomplish.

Please reply urgently.

Best regards

*Howgul Abul Arhu*

---

FROM: Dr Altaka Yurmani  
Central Bank of Nigeria  
Lagos, Nigeria  
01-658-21-2658

*Figure 40: Modern 419 Fraud*

The modern version of the advance-fee fraud usually takes place via email correspondence. Like the older version, it typically involves a promise of treasure. The "treasure" may involve a lottery jackpot, a promise of a share of a large bank account, or some other made-up story to explain why a large sum of cash will be forwarded to the victim. The criminal will also make up a plausible story to explain why a fee is needed in advance. The email may claim that a few hundred dollars are needed as an "application fee" to the contest that has purportedly already been won. Another common claim is that the wire transfer of such a large sum of money involves fees that must be paid in advance.

Criminals running 419 fraud rings use many tricks designed to lure in even skeptical targets. For example, they will send out mass mailings via the internet, but make each letter appear as though it has been received by only one individual. They may provide working phone and fax numbers to targets who demand them, and furnish documents that appear to have authentic government seals and stamps.

The Nigerian 419 Advance Fee Fraud came to the attention of the public and regulators during the 1970s over letters generally aimed at small businesses purporting to come from figures in the

Nigerian government (often the Central Bank or Nigerian National Petroleum Corporation) wanting help disposing of new oil wealth. Those letters were posted in Africa and Europe. In 2002 the US Department of Justice gained a court order to open every item of mail from Nigeria passing through JFK airport in New York, with around 70% involving scam offers. Russell Smith notes that between August and November 1998 Australia Post confiscated 4.5 tonnes of advance fee correspondence (1.8 million items) that had counterfeit postage. The 1980s and 1990s saw the scammers move from print to fax messaging followed by several explosions of email at the end of the millennium and in 2003, with the scammers spamming recipients in advanced economies (primarily those in English-speaking nations). The addressing of that email was indiscriminate, encompassing organisations and personal addresses. Today a mix of all the following approaches is used by the fast growing AFF scam rings based around the globe:

- Mail
- Fax
- Smart Phone, Apps
- E-mail
- Chat rooms, Twitter
- Dating web sites
- Matchmaking web sites
- Internet auction sites
- Social and business networking sites, Facebook, LinkedIn
- Mobile phone SMS
- Internet phone
- Internet gaming (new)
- Personal introduction
- Call centre / boiler-room

#### 4.3.5.2 Types of advance fee fraud and other Nigeria-related fraud emails

There are several variants of advance fee fraud. Some of the prominent ones are listed below:

- **Fake lottery win:** You won a lottery prize, but to receive it first you must pay various fees.
- **Company representative scam:** Some company in East Asia, Europe or Africa needs help receiving payments from customers. They need to use your bank account for cashing checks and money orders sent to you. You get to keep about 10% for forwarding the funds by *Western Union* or *MoneyGram*. Later you find out that checks had been either stolen or counterfeit and you're suddenly tens of thousands of dollars in debt to your bank.
- **Dead foreigner scam:** Some foreign owner of a bank account in Africa or Asia died without heir. If you pose as a relative, you'll get to keep a slice of this, but first you must pay various fees.



- **Unpaid contractor/Overcharged government contract:** There's an unpaid contract with an African government. If you pose as the contractor, you'll get to keep a slice of this, but first you must pay various bribes.
- **Ex-kleptocrat scam:** A family member of a former head/member of government somewhere in Africa or Asia has stashed away a few millions and seeks your help in moving it, promising you a slice of it, but first you must send money to a securities company or lawyer.
- **Murdered businessman scam:** A family member of a rich businessman in Africa who stashed away a few millions before being killed seeks your help in retrieving the inheritance, promising you a slice of it, but first you must send money to a securities company or lawyer.
- **Zimbabwean farmer scam:** A farmer or opposition politician from Zimbabwe has stashed away a few millions and seeks your help in moving it, promising you a slice of it, but first you must send money to a securities company or lawyer.
- **Dying widow scam:** A rich widow is about to die from breast cancer and wants to give you millions to use for charity, but first you must send money to her lawyer.
- **Dying rich merchant scam:** A rich merchant or oil contractor is about to die from cancer of the esophagus and wants to give you millions, but first you must send money to his lawyer.
- **Iraq scam:** A US or British soldier in Iraq has come across money or gold that Saddam Hussein had stashed away. He/she seeks your help in moving it, promising you a slice of it, but first you must send money to a securities company or lawyer.
- **Yukos oil scam:** Russian tycoon Mikhail Khodorkovsky has been arrested, but before that a few millions were stashed away. An associate seeks your help in moving it, promising you a slice of it, but first you must send money to a securities company or lawyer.
- **Diplomatic delivery scam:** Some money or valuables which you have been promised in one of the above scam formats (fake lottery, inheritance, etc) will be delivered to you by a diplomat who travelled to your country, but first you must pay money to this person (by Western Union or in cash).
- **Rich investor scam:** Some investor with lots of money wants to invest into your business or wants you to manage some funds but first you must send money to a lawyer to draw up a contract or set up a trust fund.
- **Loan scam:** Some person in Europe or Africa will lend you money at favorable conditions, but first you must send money to their lawyer or bank.
- **Credit card order:** Someone claiming to live in the USA or UK orders goods on a credit card and asks you to send them to Nigeria.
- **Oversized cashier's check:** Someone wants to buy your car, bike, horse, boat, trailer, etc. and will send you a check larger than the sticker value, asking you to wire the balance to a "shipping agent" or some other person. Other examples include apartment or holiday

home rental, purchasing land, hiring a wedding photographer, getting violin lessons, sending kids to a nanny, etc.

- **Money recovery:** A law enforcement officer (in Nigeria, FBI or elsewhere) asks you to contact them about scammers you've been dealing with. They promise to help you recover your stolen money, but first you need to send more cash.
- **Wash wash / black money:** Like "money recovery" this is not usually a scam format by itself but an element in a larger scam to maximize the amount of money stolen. You will be shown bundles of black paper the size of dollar bills, which is supposed to be cash promised in the main scam. Supposedly it was colored with black ink for security purposes and some special chemicals will restore it to its normal state and make the "money" usable, but first you need to send more cash to buy those chemicals.
- **ATM card payment scam:** This usually shows up as part of another scam, such as a fake lottery or an "unpaid contractor" scam. You will be promised an ATM card via which you can withdraw millions dollars (up to at several thousand dollars per day) at any bank worldwide, but first you need to send cash to have it mailed to you. If it arrives at all, it won't work (because there is no bank account, it's just a piece of plastic) and you'll be offered a replacement card, for a few thousand dollars more. Any money sent to the criminals by Western Union or MoneyGram is lost.
- **Job scams:** You're being offered a well-paid job in another country, but you need to start very soon and before you can do that you need to send cash to a fake immigration official or lawyer.
- **Immigration scams:** They're very similar to fake job scams. You're being told there is an easy way to immigrate to the USA or Canada (or some other country), but first you need to send cash to a fake immigration official or lawyer.
- **Fake charity/ministry:** An orphanage, pastor, NGO, etc. in an African country needs your cash.

#### 4.3.5.3 What should you do if you're a victim of 419 (Advance-fee Fraud) Scam

The guidelines one must follow, in case he/she is a victim of 419 scam is as follows:

- Report it to Action Fraud.
- End all further contact with the fraudsters at once.
- Don't send them any more money.
- If you have given the fraudsters your bank account details, contact your bank immediately.
- If the fraudsters threaten you once you stop co-operating with them, tell the police immediately.
- Send a copy of the original email to both your own Internet Service Provider (ISP) and the ISP of the sender. Address it to 'abuse@' followed by the email address.

- Be aware that you will probably be targeted for other frauds. Fraudsters frequently pass on the details of people they have successfully targeted to other fraudsters. Or, they may approach the victim under different names to commit further frauds.
- Often people who have already lost money to fraudsters fall victim to fraud recovery fraud. Here, fraudsters contact victims pretending to be law enforcement specialists or lawyers. They reassure the victim that they can help to recover their lost money – but they also ask for a fee.

#### 4.3.5.4 Protection Tips

- The first question to ask yourself is "why me?" This person doesn't know you and has no reason to trust you. The best way to deal with an e-mail like this is to delete it straight away.
- Governments and large corporations do not transfer money through another person's bank account. Any suggestion that they do so is a reliable indication that you have been approached by fraudsters.
- Letters and documents sent by fraudsters are usually badly written. Look out for spelling mistakes and poor grammar.
- If a deal seems to be too good to be true, then it probably is.
- Beware of being told you must act quickly or you'll miss out on this 'one-time deal'.
- Never send your bank or personal details. If you have done, contact your bank immediately to stop money being withdrawn and sent overseas.
- Never send any money.
- Never, under any circumstances, travel anywhere in response to one of these scams. You won't see your money again, and you could put yourself in physical danger.

#### 4.3.5.5 Case Studies on 419 Scam

##### *Case I: 11 people arrested for net-banking, lottery fraud*

The arrest was made by the Cyber Crime Cell of Economic Offences Wing (EOW) of Delhi Police. As per media reports, these people operated as a team. The Nigerian nationals would hack the user id and password of various bank accounts of Indians and then pass on the information to Indian members of attackers team. These accounts used to be on fake identities or of people who agreed to lend their accounts to attackers on commission. In this case, the account holder provided ATM cards with PIN of such accounts to attackers for withdrawal of the fraudulent money, police said.

Crime came under the scanner after Director of Siddharth Polychem India Pvt. Ltd lodged a complaint on May 6 alleging that 27 unauthorised online transactions were done some unknown persons from his company's bank account in which around Rs 53 lakh were siphoned off into 12 different bank accounts of different cities across India, police said.

##### *Case II: 5 Nigerian arrested for involvement in inter-state job racket*

Mumbai police arrested 5 Nigerian nationals for their involvement in an International job scam. They used to send bulk emails to the people and offer jobs abroad in hotel industry. If anyone fell prey in their trap, they use to ask them to transfer consultancy fee in their Mumbai bank account. Once the payment is made, these people use to disappear and never contact them back. This incident came to light when Mr. Prabhat Singh from Orrisa lodged a complaint against them in the Juhu police station stating that he had made a payment of Rs 1.20 lakhs to some unidentified person, who contacted him through email and introduced him as a job agent, as a consultancy fee for a job in a hotel located in UK. The consultant vanished once the payment was made. The culprits were traced by police through the bank account details, mobile number and email-id that were used by the criminals.

### **4.3.6 Unexpected prize and lottery**

Unexpected prize and lottery scams work by asking you to pay some sort of fee in order to claim your prize or winnings from a competition or lottery you never entered. You will receive notification that you have won a lot of money or a fantastic prize in a competition, lottery or sweepstake that you don't remember entering. The contact may come by mail, telephone, email, text message or social media. The prize you have 'won' could be anything from a tropical holiday to electronic equipment such as a laptop or a smartphone, or even money from an international lottery. To claim your prize, you will be asked to pay a fee. Scammers will often say these fees are for insurance costs, government taxes, bank fees or courier charges. The scammers make money by continually collecting these fees from you and stalling the payment of your winnings.

Alternatively the scammer will collect a premium rate on the phone number you are asked to dial (usually starting with 190). They will try to keep you on the line for a long time in order to clock up a hefty charge, and may even ask you to call a second premium rate number.

The email, letter or text message you receive will ask you to respond quickly or risk missing out. It may also urge you to keep your winnings private or confidential, to 'maintain security' or stop other people from getting your prize by mistake. Scammers do this to prevent you from seeking further information or advice from independent sources.

Lottery scams may use the names of legitimate overseas lotteries (often Spanish lotteries), so that if you do some superficial research, the scam will seem real. Some examples of the real Spanish lotteries that the scammers falsely use are Loteria Primitiva and El Gordo.

You may also be asked to provide personal details to prove that you are the correct winner and to give your bank account details so the prize can be sent to you. Scammers use these details to try to misuse your identity and steal any money you have in your bank account.

Sometimes the scammers actually do send a cheque for part of your winnings, such as a few thousand dollars of winnings, to trick you into thinking the offer is legitimate. However this cheque will eventually bounce and you will not receive any real payments.

The scammer will take your payment and fail to deliver the prize, or send you something that falls short of the promised prize.

**Case I :** Nicole was browsing the internet when a pop-up message appeared on her screen informing her that she had won a holiday to the Bahamas. To claim her prize she would have to call the number listed within three minutes. Nicole immediately called the number. A female voice with an American accent answered the call and told Nicole in an excited voice that she'd won the holiday.

'The woman who answered the phone spoke very quickly and I was quite excited about the prospect of a holiday. When she asked me if I accepted the holiday, I immediately said "yes". I was very excited and my adrenaline was right up,' Nicole explained.

The woman mentioned some figures that didn't seem to have any connection to the holiday prize, and asked Nicole for her credit card details. It wasn't until she asked for these details that Nicole began to suspect that she had not really won an all-expenses-paid holiday package. After the woman had taken Nicole's credit card details, she told Nicole that she was 'locked in' to buying the holiday. Nicole panicked when she heard the term 'locked in' as she and her husband are both students. Once she realised that part of the holiday cost had been charged to her credit card, Nicole asked to withdraw but the woman on the phone refused. Eventually, Nicole spoke to a manager who also refused to let Nicole cancel the agreement to purchase the holiday package.

Nicole said that by this stage 'I was almost crying and I was very upset'. Nicole was told that if she didn't calm down they wouldn't help her at all. After this, the manager said, 'We'll take the amount you have to pay down from \$680 to \$350 (US) and you can try and sell the holiday to someone else.'

The manager also told Nicole that she had to listen to a recording of the company's terms and conditions and confirm that she understood and agreed to them. Nicole was still upset and asked if she could wait until her husband was there before she listened or agreed to anything. However, the manager told Nicole that if she hung up the phone, she would have to pay \$1,000 (US) and she would be charged double if she made a complaint. Nicole reluctantly agreed to listen to the recorded terms and conditions.

'I agreed to the terms and conditions even though I was too upset to understand what they were really saying.'

The company selling the holiday used high pressure tactics to force Nicole into a transaction she didn't really understand. Nicole said that 'it was abuse, full tilt abuse. They were so rude to me.' After Nicole got off the phone with the holiday people, she contacted her bank and cancelled her credit card and the bank said they would do their best to get the money back. 'My husband spent hours on the internet looking for these people and trying to contact them. Eventually we made contact and the person from the company was extremely apologetic and promised a full refund,' Nicole said. However, the next day when they contacted Nicole again, they gave her a false

telephone number. Even though Nicole's bank managed to get her money back, this scam caused Nicole and her husband a lot of stress and inconvenience.

### **macS ecnamoR dna gnitaD 4.3.7**

Scammers take advantage of people looking for romantic partners, often via dating websites, apps or social media by pretending to be prospective companions. They play on emotional triggers to get you to provide money, gifts or personal details.

Dating and romance scams often take place through online dating websites, but scammers may also use social media or email to make contact. They have even been known to telephone their victims as a first introduction. These scams are also known as 'catfishing'. Scammers typically create fake online profiles designed to lure you in. They may use a fictional name, or falsely take on the identities of real, trusted people such as military personnel, aid workers or professionals working abroad. Dating and romance scammers will express strong emotions for you in a relatively short period of time, and will suggest you move the relationship away from the website to a more private channel, such as phone, email or instant messaging. They often claim to be from Australia or another western country, but travelling or working overseas.

Scammers will go to great lengths to gain your interest and trust, such as showering you with loving words, sharing 'personal information' and even sending you gifts. They may take months to build what may feel like the romance of a lifetime and may even pretend to book flights to visit you, but never actually come. Once they have gained your trust and your defences are down, they will ask you (either subtly or directly) for money, gifts or your banking/credit card details. They may also ask you to send pictures or videos of yourself, possibly of an intimate nature. Often the scammer will pretend to need the money for some sort of personal emergency. For example, they may claim to have a severely ill family member who requires immediate medical attention such as an expensive operation, or they may claim financial hardship due to an unfortunate run of bad luck such as a failed business or mugging in the street. The scammer may also claim they want to travel to visit you, but cannot afford it unless you are able to lend them money to cover flights or other travel expenses. Sometimes the scammer will send you valuable items such as laptop computers and mobile phones, and ask you to resend them somewhere. They will invent some reason why they need you to send the goods but this is just a way for them to cover up their criminal activity. Alternatively they may ask you to buy the goods yourself and send them somewhere. You might even be asked to accept money into your bank account and then transfer it to someone else.

Sometimes the scammer will tell you about a large amount of money or gold they need to transfer out of their country, and offer you a share of it. They will tell you they need your money to cover administrative fees or taxes.

Dating and romance scammers can also pose a risk to your personal safety as they are often part of international criminal networks. Scammers may attempt to lure their victims overseas, putting you in dangerous situations that can have tragic consequences.

Regardless of how you are scammed, you could end up losing a lot of money. Online dating and romance scams cheat Australians out of millions every year. The money you send to scammers is almost always impossible to recover and, in addition, you may feel long-lasting emotional betrayal at the hands of someone you thought loved you.

**Case I :** He does not know much about computer hacking, yet 51-year-old cyber criminal Pranab Mitra has stunned even the cyber crime investigation cell of Mumbai police with his bizarre fraud on the Net. Mitra, a former executive of Gujarat Ambuja Cement, was arrested on Monday for posing as a woman and seducing online an Abu Dhabi-based man, thereby managing to extort Rs 96 lakh from him. Investigating officer, Assistant Commissioner of Police, J.S. Sodi, said Mitra has been remanded to police custody till June 24, and has been booked for cheating, impersonation, blackmail and extortion under sections 420, 465, 467, 471, 474 of the IPC, read with the newly formed Information Technology Act.

Mitra posed as a woman, Rita Basu, and created a fake e-mail ID through which he contacted one V.R. Ninawe. According to the FIR, Mitra trapped Ninawe in a “cyber-relationship” sending emotional messages and indulging in online sex since June 2002. Later, Mitra sent an e-mail that “she would commit suicide” if Ninawe ended the relationship. He also gave him “another friend Ruchira Sengupta’s” e-mail ID which was in fact his second bogus address. When Ninawe mailed at the other ID he was shocked to learn that Mitra had died. Then Mitra began the emotional blackmail by calling up Abu Dhabi to say that police here were searching for Ninawe. Ninawe panicked on hearing the news and asked Mitra to arrange for a good advocate for his defence. Ninawe even deposited a few lakh in the bank as advocate fees. Mitra even sent e-mails as high court and police officials to extort more money. Ninawe finally came down to Mumbai to lodge a police case.

**Case II:** Mumbai based software engineer was cheated by a Trivendrum based 27 year old boy Rajesh posing as a women over Internet. Rajesh disguised as Renuka and become friend with the software engineer . They use to voice chat over internet , where Rajesh used voice converter software to disguise female voice . Rajesh forwarded a photo from a marriage bureau to the engineer, who provided a credit card and code to ‘Renuka’ to withdraw Rs . 2500 for purchasing a flight ticket to Mumbai . After receiving the credit card number and the CCV code , Rajesh withdrew Rs. 22,000 from the credit card . Later the victim lodged the complaint and the Rajesh was trapped by the police.

#### ***4.4 LET US SUM UP***

In this unit we discussed and analyzed various type of cyber crimes, techniques adopted by the attackers and the case studies. Unit also discussed about the prevention tips for users. It should

be noted that awareness of the users of technology is vital in defending against the cyber crime and cyber attacks.

#### ***4.5 CHECK YOUR PROGRESS***

1. What is 419 fraud?
2. APWG Stands for .....
3. What is a single best method of protection against cyber crimes.
4. NCRB Stands for .....
5. Phistank.com is a .....

#### ***4.6 ANSWERS TO CHECK YOUR PROGRESS***

1. Advance fee fraud scam visit 4.3.5 for more details
2. APWG Stands for Anti-Phishing Working Group
3. What is a single best method of protection against cyber crimes: User Awareness
4. NCRB Stands for National Crime Records Bureau
5. Phistank.com is a collaborative clearing house for data and information about phishing on the Internet.

#### ***4.7 MODEL QUESTIONS***

1. Write a short note on Phishing attacks.
2. Discuss some of the phishing incidents.
3. What is Nigerian fraud?
4. Explain prevention tips for cyber stalking.
5. What is fast-flux?
6. Define DNS Phishing?
7. What is Deep web?
8. Define Ransomware?
9. What is cyptoLocker?
10. What is keylogging?

Activity 1 : Look at the spam messages received by you for possible traces and intention of cyber criminal.

Activity 2 : Visit <https://www.phishtank.com/> and browse through the contents of site and collect information.



## **BLOCK III**

# UNIT I: INFORMATION SECURITY

## ***1.1 LEARNING OBJECTIVES***

After going through this unit you will be able to:

- Define Security
- Understand Models for Discussing Security Issues
- Understand possible kind of attacks
- Know Defense in Depth

## ***1.2 INTRODUCTION***

Information security is a concept that becomes ever more enmeshed in many aspects of our society, largely as a result of our nearly ubiquitous adoption of computing technology. In our everyday lives, many of us work with computers for our employers, play on computers at home, go to school online, buy goods from merchants on the Internet, take our laptops to the coffee shop and check our e-mail carry our smart phones on our hips and use them to check our bank balances, track our exercise with sensors in our shoes, and so on, ad infinitum. Although this technology enables us to be more productive and allows us to access a host of information with only a click of the mouse, it also carries with it a host of security issues. If the information on the systems used by our employers or our banks becomes exposed to an attacker, the consequences can be dire indeed. We could suddenly find ourselves bereft of funds, as the contents of our bank account are transferred to a bank in another country in the middle of the night. Our employer could lose millions of dollars, face legal prosecution, and suffer damage to its reputation because of a system configuration issue allowing an attacker to gain access to a database containing Personally Identifiable Information (PII) or proprietary information. We see such issues appear in the media with disturbing regularity. If we look back 30 years, such issues related to computer systems were nearly nonexistent, largely due to the low level of technology and the few people who were using what was in place. Although technology changes at an increasingly rapid rate, and specific implementations arise on a seemingly daily basis, much of the theory that discusses how we go about keeping ourselves secure changes at a much slower pace and does not always keep up with the changes to our technology. If we can gain a good understanding of the basics of information security, we are on a strong footing to cope with changes as they come along.

## ***1.3WHAT IS INFORMATION SECURITY?***

Sometimes referred to as computer security, Information Technology security is information security applied to technology (most often some form of computer system). It is worthwhile to note that a computer does not necessarily mean a home desktop. A computer is any device with a processor and some memory. Such devices can range from non-networked standalone devices as simple as calculators, to networked mobile computing devices such as smartphones and tablet

computers. IT security specialists are almost always found in any major enterprise/establishment due to the nature and value of the data within larger businesses. They are responsible for keeping all of the technology within the company secure from malicious cyber attacks that often attempt to breach into critical private information or gain control of the internal systems.

Information security is defined as *"protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction"*. In essence, it means we want to protect our data and our systems from those who would seek to misuse it. In a general sense, security means protecting our assets. This may mean protecting them from attackers invading our networks, natural disasters, adverse environmental conditions, power failures, theft or vandalism, or other undesirable states. Ultimately, we will attempt to secure ourselves against the most likely forms of attack, to the best extent we reasonably can, given our environment.

When we look at what exactly it is that we secure, we may have a broad range of potential assets. We can consider physical items that we might want to secure, such as those of inherent value (e.g., gold bullion) or those that have value to our business (e.g., computing hardware). We may also have items of a more ethereal nature, such as software, source code, or data. In today's computing environment, we are likely to find that our logical assets are at least as valuable as, if not more than, our physical assets. Additionally, we must also protect the people who are involved in our operations. People are our single most valuable asset, as we cannot generally conduct business without them. We duplicate our physical and logical assets and keep backup copies of them elsewhere against catastrophe occurring, but without the skilled people to operate and maintain our environments, we will swiftly fail. In our efforts to secure our assets, we must also consider the consequences of the security we choose to implement. There is a well-known quote that says, *"The only truly secure system is one that is powered off, cast in a block of concrete and sealed in a lead-lined room with armed guards- and even then I have my doubts"*. Although we could certainly say that a system in such a state could be considered reasonably secure, it is surely not usable or productive. As we increase the level of security, we usually decrease the level of productivity. With the system mentioned in quote above, the level of security would be very high, but the level of productivity would be near zero.

Additionally, when securing an asset, system, or environment, we must also consider how the level of security relates to the value of the item being secured. We can, if we are willing to accommodate the decrease in performance, apply very high levels of security to every asset for which we are responsible. We can build a billion-dollar facility surrounded by razor wire fences and patrolled by armed guards and vicious attack dogs, and carefully place our asset in a hermetically sealed vault inside ... so that it is not possible for an insect to sneak-in, but that would not make any sense. In some environments, however, such security measures might not be enough. In any environment where we plan to put

heightened levels of security in place, we also need to take into account the cost of replacing our assets if we do happen to lose them, and make sure we establish reasonable levels of protection for their value. The cost of the security we put in place should never outstrip the value of what it is protecting.

### 1.3.1 Various Definitions

The definitions of Information Security suggested in different sources are summarized below<sup>69</sup>:

1. "Preservation of confidentiality, integrity and availability of information. Note: In addition, other properties, such as authenticity, accountability, non-repudiation and reliability can also be involved." (ISO/IEC 27000:2009)
2. "The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability." (CNSS, 2010)
3. "Ensures that only authorized users (confidentiality) have access to accurate and complete information (integrity) when required (availability)." (ISACA, 2008)
4. "Information Security is the process of protecting the intellectual property of an organisation." (Pipkin, 2000)
5. "...information security is a risk management discipline, whose job is to manage the cost of information risk to the business." (McDermott and Geer, 2001)
6. "A well-informed sense of assurance that information risks and controls are in balance." (Anderson, J., 2003)
7. "Information security is the protection of information and minimises the risk of exposing information to unauthorised parties." (Venter and Eloff, 2003)
8. "Information Security is a multidisciplinary area of study and professional activity which is concerned with the development and implementation of security mechanisms of all available types (technical, organisational, human-oriented and legal) in order to keep information in all its locations (within and outside the organisation's perimeter) and, consequently, information systems, where information is created, processed, stored, transmitted and destroyed, free from threats.

Threats to information and information systems may be categorised and a corresponding security goal may be defined for each category of threats. A set of security goals, identified as a result of a threat analysis, should be revised periodically to ensure its adequacy and conformance with the evolving environment. The currently relevant set of security goals may include: confidentiality, integrity, availability, privacy, authenticity & trustworthiness, non-repudiation, accountability and auditability.

---

<sup>69</sup> [https://en.wikipedia.org/wiki/Information\\_security](https://en.wikipedia.org/wiki/Information_security)

### 1.3.2 Information assurance

It is the act of ensuring that data is not lost when critical issues arise. These issues include, but are not limited to: natural disasters, computer/server malfunction, physical theft, or any other instance where data has the potential of being lost. Since most information is stored on computers in our modern era, information assurance is typically dealt with by IT security specialists. One of the most common methods of providing information assurance is to have an off-site backup of the data in case one of the mentioned issues arise.

### 1.3.3 When Are We Secure?

Defining the exact point at which we can be considered secure presents a bit of a challenge.

- Are we secure if our systems are properly patched?
- Are we secure if we use strong passwords?
- Are we secure if we are disconnected from the Internet entirely?

Even from common-sense, all of these questions can be answered with a "no." Even if our systems are properly patched, there will always be new attacks to which we are vulnerable. When strong passwords are in use, there will be other avenues that an attacker can exploit. When we are disconnected from the Internet, our systems can be physically accessed or stolen. In short, it is very difficult to define when we are truly secure. We can, however, turn the question around. Defining when we are **insecure** is a much easier task, and we can quickly list a number of items that would put us in this state:

- Not patching our systems
- Using weak passwords such as "password" or "1234"
- Downloading programs from the Internet
- Opening e-mail attachments from unknown senders
- Using wireless networks without encryption

We could go on for some time creating such a list. The good thing is that once we are able to point out the areas in an environment that can cause it to be insecure, we can take steps to mitigate these issues. This problem is akin to cutting something in half over and over; there will always be some small portion left to cut again. Although we may never get to a state that we can definitively call "100 percent secure", we can take steps in the right direction.

The bodies of law that define standards for security, vary quite a bit from one industry to another and wildly from one country to another. Organizations that operate globally are very common at present, and we need to take care that we are not violating any such laws in the course of conducting business. We can see exactly such a case when we look at the differences in data privacy laws between the United States and the European Union. When in doubt, consult legal counsel before acting. Some bodies of law or regulations do make an attempt to define what secure is, or at least some of the steps we should take to be "secure enough." We have the Payment Card Industry Data Security Standard (PCI DSS) for companies that process credit card payments, the Health Insurance Portability and Accountability Act of 1996 (HIPAA)

for organizations that handle health care and patient records, the Federal Information Security Management Act (FISMA) that defines security standards for many federal agencies in the United States, and a host of others. Whether these standards are effective or not is the source of much discussion, but following the security standards defined for the industry in which we are operating is generally considered to be advisable, if not mandated.

## ***1.4 MODELS FOR DISCUSSING SECURITY ISSUES***

When we discuss security issues, it is often helpful to have a model that we can use as a foundation or a baseline. This gives us a consistent set of terminology and concepts that we, as security professionals, can refer to when security issues arise.

### **1.4.1 The Confidentiality, Integrity and Availability Triad**

Three of the primary concepts in information security are confidentiality, integrity, and availability, commonly known as the confidentiality, integrity, and availability (CIA) triad. The CIA triad gives us a model by which we can think about and discuss security concepts, and tends to be very focused on security, as it pertains to data. The common notation for confidentiality, integrity, and availability is CIA. In certain materials, largely those developed by ISC2 we may see this rearranged slightly as CAI. No change to the concepts is implied in this rearrangement, but it can be confusing for those who do not know about it in advance. We may also see the CIA concepts expressed in their negative forms: i.e disclosure, alteration, and denial (DAD).

#### **1.4.1.1 Confidentiality**

In information security, confidentiality *"is the property, that information is not made available or disclosed to unauthorized individuals, entities, or processes"* (Excerpt ISO27000). Confidentiality is a concept similar to, but not the same as, privacy. Confidentiality is a necessary component of privacy and refers to our ability to protect our data from those who are not authorized to view it. Confidentiality is a concept that may be implemented at many levels of a process. As an example, if we consider the case of a person withdrawing money from an ATM, the person in question will likely seek to maintain the confidentiality of the personal identification number (PIN) that allows him, in combination with his ATM card, to draw funds from the ATM. Additionally, the owner of the ATM will hopefully maintain the confidentiality of the account number, balance, and any other information needed to communicate to the bank from which the funds are being drawn. The bank will maintain the confidentiality of the transaction with the ATM and the balance change in the account after the funds have been withdrawn. If at any point in the transaction confidentiality is compromised, the results could be bad for the individual the owner of the ATM, and the bank, potentially resulting in what is known in the information security field as a breach.

Confidentiality can be compromised by the loss of a laptop containing data, a person looking over our shoulder while we type a password, an e-mail attachment being sent to the wrong person, an attacker penetrating our systems, or similar issues.

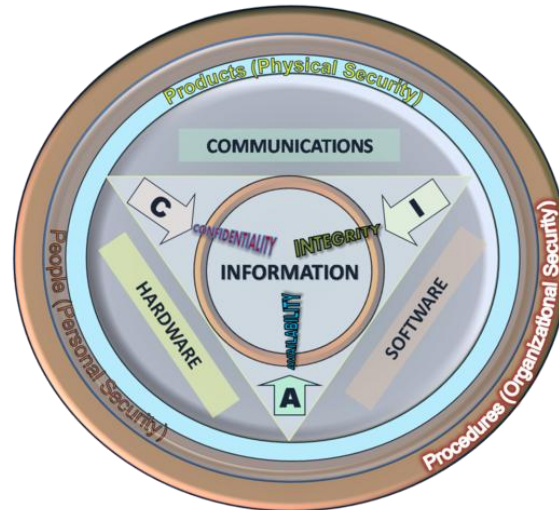


Figure 41: The CIA Triad<sup>70</sup>

#### 1.4.1.2 Integrity

Integrity refers to the ability to prevent our data from being changed in an unauthorized or undesirable manner. This could mean the unauthorized change or deletion of our data or portions of our data, or it could mean an authorized, but undesirable, change or deletion of our data. To maintain integrity, we not only need to have the means to prevent unauthorized changes to our data but also need the ability to reverse authorized changes that need to be undone. We can see a good example of mechanisms that allow us to control integrity in the file systems of many modern operating systems such as Windows and Linux. For purposes of preventing unauthorized changes, such systems often implement permissions that restrict what actions an unauthorized user can perform on a given file. Additionally, some such systems, and many applications, such as databases, can allow us to undo or roll back changes that are undesirable. Integrity is particularly important when we are discussing the data that provides the foundation for other decisions. If an attacker were to alter the data that contained the results of medical tests, we might see the wrong treatment prescribed, potentially resulting in the death of the patient.

#### 1.4.1.2 Availability

The final leg of the CIA triad is availability. Availability refers to the ability to access our data when we need it. Loss of availability can refer to a wide variety of breaks anywhere in the chain that allows us access to our data. Such issues can result from power loss, operating system or application problems, network attacks, compromise of a system, or other problems. When such

<sup>70</sup> <https://en.wikipedia.org/wiki/File:CIAJMK1209.png>

issues are caused by an outside party, such as an attacker, they are commonly referred to as a denial of service (DoS) attack.

### 1.4.2 Relating the CIA triad to security

Given the elements of the CIA triad, we can begin to discuss security issues in a very specific fashion. As an example, we can look at a shipment of backup tapes on which we have the only existing, but unencrypted, copy of some of our sensitive data stored. If we were to lose the shipment in transit we will have a security issue. From a confidentiality standpoint, we are likely to have a problem since our files were not encrypted. From an integrity standpoint, presuming that we were able to recover the tapes, we again have an issue due to the lack of encryption used on our files. If we recover the tapes and the unencrypted files were altered, this would not be immediately apparent to us. As for availability, we have an issue unless the tapes are recovered since we do not have a backup copy of the files. Although we can describe the situation in this example with relative accuracy using the CIA triad, we might find that the model is more restrictive than what we need in order to describe the entire situation. An alternative model does exist that is somewhat more extensive.

## 1.5 THE PARKERIAN HEXAD

The Parkerian hexad, named for Donn Parker and introduced in his book *Fighting Computer Crime*, provides us with a somewhat more complex variation of the classic CIA triad. Where the CIA triad consists of confidentiality, integrity, and availability, the Parkerian hexad consists of these three principles, as well as possession or control, authenticity, and utility for a total of six principles, as shown in Figure 42 below. Although it is considered by some to be a more complete model, the Parkerian hexad is not as widely known as the CIA triad. If we decide to use this model in discussion of a security situation, we should be prepared to explain the difference to the uninitiated.



Figure 42: The Parkerian hexad



### **1.5.1 Confidentiality, Integrity and Availability**

As we mentioned, the Parkerian hexad encompasses the three principles of the CIA triad with the same definitions we just discussed. There is some variance in how Parker describes integrity, as he does not account for authorized, but incorrect, modification of data, and instead focuses on the state of the data itself in the sense of completeness.

### **1.5.2 Possession or Control**

Possession or control refers to the physical disposition of the media on which the data is stored. This enables us, without involving other factors such as availability, to discuss our loss of the data in its physical medium. In our lost shipment of backup tapes, let us say that some of them were encrypted and some of them were not. The principle of possession would enable us to more accurately describe the scope of the incident; the encrypted tapes in the lot are a possession problem but not a confidentiality problem, and the unencrypted tapes are a problem on both counts.

### **1.5.3 Authenticity**

Authenticity allows us to talk about the proper attribution as to the owner or creator of the data in question. For example, if we send an e-mail message that is altered so as to appear to have come from a different e-mail address than the one from which it was actually sent, we would be violating the authenticity of the e-mail. Authenticity can be enforced through the use of digital signatures. A very similar, but reversed, concept to this is non-repudiation. Nonrepudiation prevents someone from taking an action, such as sending an e-mail, and then later denying that he or she has done so.

### **1.5.4 Utility**

Utility refers to how useful the data is to us. Utility is also the only principle of the Parkerian hexad that is not necessarily binary in nature; we can have a variety of degrees of utility, depending on the data and its format. This is a somewhat abstract concept, but it does prove useful in discussing certain situations in the security world. For instance, in one of our earlier examples we had a shipment of backup tapes, some of which were encrypted and some of which were not. For an attacker, or other unauthorized person, the encrypted tapes would likely be of very little utility, as the data would not be readable. The unencrypted tapes would be of much greater utility, as the attacker or unauthorized person would be able to access the data.

## ***1.6 ATTACKS***

We may face attacks from a wide variety of approaches and angles. When we look at what exactly makes up an attack, we can break it down according to the type of attack that it represents, the risk the attack represents, and the controls we might use to mitigate it.

### **1.6.1 Types of Attacks**

When we look at the types of attacks we might face, we can generally place them into one of four categories: interception, interruption, modification, and fabrication. Each category can affect one or more of the principles of the CIA triad, as shown in Figure 43 below. Additionally, the

lines between the categories of attack and the particular effects they can have are somewhat blurry. Depending on the attack in question, we might argue for it to be included in more than one category, or have more than one type of effect.

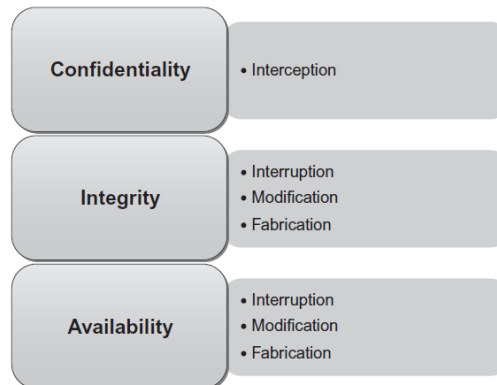


Figure 43: Category of CIA triad

### 1.6.1.1 Interception

Interception attacks allow unauthorized users to access our data, applications, or environments, and are primarily an attack against confidentiality. Interception might take the form of unauthorized file viewing or copying, eavesdropping on phone conversations, or reading e-mail, and can be conducted against data at rest or in motion. Properly executed, interception attacks can be very difficult to detect.

### 1.6.1.2 Interruption

Interruption attacks cause our assets to become unusable or unavailable for our use, on a temporary or permanent basis. Interruption attacks often affect availability but can be an attack on integrity as well. In the case of a DoS attack on a mail server, we would classify this as an availability attack. In the case of an attacker manipulating the processes on which a database runs in order to prevent access to the data it contains, we might consider this an integrity attack, due to the possible loss or corruption of data, or we might consider it a combination of the two. We might also consider such a database attack to be a modification attack rather than an interruption attack.

### 1.6.1.3 Modification

Modification attacks involve tampering with our asset. Such attacks might primarily be considered an integrity attack but could also represent an availability attack. If we access a file in an unauthorized manner and alter the data it contains, we have affected the integrity of the data contained in the file. However, if we consider the case where the file in question is a configuration file that manages how a particular service behaves, perhaps one that is acting as a Web server, we might affect the availability of that service by changing the contents of the file. If we continue with this concept and say the configuration we altered in the file for our Web server is one that alters how the server deals with encrypted connections, we could even make this a confidentiality attack.

#### **1.6.1.4 Fabrication**

Fabrication attacks involve generating data, processes, communications, or other similar activities with a system. Fabrication attacks primarily affect integrity but could be considered an availability attack as well. If we generate spurious information in a database, this would be considered to be a fabrication attack. We could also generate e-mail, which is commonly used as a method for propagating malware, such as we might find being used to spread a worm. In the sense of an availability attack, if we generate enough additional processes, network traffic, e-mail, Web traffic, or nearly anything else that consumes resources, we can potentially render the service that handles such traffic unavailable to legitimate users of the system.

### ***1.7 THREATS, VULNERABILITIES AND RISK***

In order to be able to speak more specifically on attacks, we need to introduce a few new items of terminology. When we look at the potential for a particular attack to affect us, we can speak of it in terms of threats, vulnerabilities, and the associated risk that might accompany them.

#### **1.7.1 Threats**

When we spoke of the types of attacks we might encounter, in the "Attacks" earlier in this chapter, we discussed some of the things that have the potential to cause harm to our assets. Ultimately, this is what a threat is—something that has the potential to cause us harm. Threats tend to be specific to certain environments, particularly in the world of information security. For example, although a virus might be problematic on a Windows operating system, the same virus will be unlikely to have any effect on a Linux operating system.

#### **1.7.2 Vulnerabilities**

Vulnerabilities are weaknesses that can be used to harm us. In essence, they are holes that can be exploited by threats in order to cause us harm. A vulnerability might be a specific operating system or application that we are running, a physical location where we have chosen to place our office building, a data center that is populated over the capacity of its air-conditioning system, a lack of backup generators, or other factors.

#### **1.7.3 Risk**

Risk is the likelihood that something bad will happen. In order for us to have a risk in a particular environment, we need to have both a threat and a vulnerability that the specific threat can exploit. For example, if we have a structure that is made from wood and we set it on fire, we have both a threat (the fire) and a vulnerability that matches it (the wood structure). In this case, we most definitely have a risk. Likewise, if we have the same threat of fire, but our structure is made of concrete, we no longer have a credible risk, because our threat does not have a vulnerability to exploit. We can argue that a sufficiently hot flame could damage the concrete, but this is a much less likely event. We will often have similar discussions regarding potential risk in computing environments, and potential, but unlikely, attacks that could happen. In such cases, the best strategy is to spend our time mitigating the most likely

attacks. If we sink our resources into trying to plan for every possible attack, however unlikely, we will spread ourselves thin and will be lacking in protection where we actually need it the most.

### **1.7.4 Impact**

Some organizations, such as the U.S. National Security Agency (NSA), add an additional factor to the threat/vulnerability/risk equation, in the form of impact. If we consider the value of the asset being threatened to be a factor, this may change whether we see a risk as being present or not. If we revisit our example of lost backup tape and stipulate that the unencrypted backup tapes contain only our collection of chocolate chip cookie recipes, we may not actually have a risk. The data being exposed would not cause us a problem, as there was nothing sensitive in it and we can make additional backups from the source data. In this particular case, we might safely say that we have no risk.

## **1.8 CONTROLS**

In order to help us mitigate risk we can put measures in place to help ensure that a given type of threat is accounted for. These measures are referred to as controls. Controls are divided into three categories: physical, logical and administrative.

### **1.8.1 Physical**

Physical controls are those controls that protect the physical environment in which our systems sit or where our data is stored. Such controls also control access in and out of such environments. Physical controls logically include items such as fences, gates, locks, bollards, guards, and cameras, but also include systems that maintain the physical environment such as heating and air conditioning systems, fire suppression systems, and backup power generators. Although at first glance, physical controls may not seem like they would be integral to information security, they are actually one of the more critical controls with which we need to be concerned. If we are not able to physically protect our systems and data, any other controls that we can put in place become irrelevant. If an attacker is able to physically access our systems, he can, at the very least steal or destroy the system, rendering it unavailable for our use in the best case. In the worst case, he will have access directly to our applications and data and will be able to steal our information and resources, or subvert them for his own use.

### **1.8.2 Logical**

Logical controls, sometimes called technical controls, are those that protect the systems, networks, and environments that process, transmit and store our data. Logical controls can include items such as passwords, encryption, logical access controls, firewalls, and intrusion detection systems. Logical controls enable us, in a logical sense, to prevent unauthorized activities from taking place. If our logical controls are implemented properly and are successful an attacker or unauthorized user cannot access our applications and data without subverting the controls that we have in place.

### **1.8.3 Administrative**

Administrative controls are based on rules, laws, policies, procedures, guidelines, and other items that are “paper” in nature. In essence, administrative controls set out the rules for how we expect the users of our environment to behave. Depending on the environment and control in question, administrative controls can represent differing levels of authority. We may have a simple rule such as “turn the coffee pot off at the end of the day,” aimed at ensuring that we do not cause a physical security problem by burning our building down at night. We may also have a more stringent administrative control, such as one that requires us to change our password every 90 days.

One important concept when we discuss administrative controls is the ability to enforce compliance with them. If we do not have the authority or the ability to ensure that our controls are being complied with, they are worse than useless, because they create a false sense of security. For example, if we create a policy that says our business resources cannot, in any fashion, be used for personal use, we need to be able to enforce this. Outside of a highly secure environment, this can be a difficult task. We will need to monitor telephone and mobile phone usage, Web access, e-mail use, instant message conversations, installed software, and other potential areas for abuse. Unless we were willing to devote a great deal of resources for monitoring these and other areas, and dealing with violations of our policy, we would quickly have a policy that we would not be able to enforce. Once it is understood that we do not enforce our policies, we can quickly set ourselves up for a bad situation.

## ***1.9 DEFENSE IN DEPTH***

Defense in depth is a strategy common to both military maneuvers and information security. In both senses, the basic concept of defense in depth is to formulate a multilayered defense that will allow us to still mount a successful defense should one or more of our defensive measures fail. In Figure 44, we can see an example of the layers we might want to put in place to defend our assets from a logical perspective; we would at the very least want defenses at the external network, internal network, host, application, and data levels. Given well-implemented defenses at each layer, we will make it very difficult to successfully penetrate deeply into our network and attack our assets directly.

One important concept to note when planning a defensive strategy using defense in depth is that it is not a magic bullet. No matter how many layers we put in place, or how many defensive measures we place at each layer, we will not be able to keep every attacker out for an indefinite period of time, nor is this the ultimate goal of defense in depth in an information security setting. The goal is to place enough defensive measures between our truly important assets and the attacker so that we will both notice that an attack is in progress and also buy ourselves enough time to take more active measures to prevent the attack from succeeding.

We can see exactly such a strategy in the theatre release of the Batman movie, *The Dark Knight*, in 2008. The production company for the movie, Warner Bros., spent six months developing

a multilayered defensive strategy to keep the movie from being pirated and placed on file-sharing networks for as long as possible. These measures included a tracking system to monitor who had access to copies of the movie at any given time, shipping the film reels in multiple parts separately to theaters in order to keep the entire movie from being stolen in shipping, monitoring movie theaters with night-vision equipment to watch for those attempting to record the movie in the theater, and other measures. Despite all the time and resources spent to prevent piracy of the movie, it was found on a file-sharing network 38 hours after it was released. For Warner Bros., this was considered a success, as the company was able to prevent the movie from being pirated for a long enough period that opening weekend sales were not significantly impacted.

### 1.9.1 Layers

When we look at the layers we might place in our defense in depth strategy, we will likely find that they vary given the particular situation and environment we are defending. As we discussed, from a strictly logical information security perspective, we would want to look at the external network, network perimeter, internal network host, application, and data layers as areas to place our defenses. We could add complexity to our defensive model by including other vital layers such as physical defenses, policies, user awareness and training, and a multitude of others, but we will stay with a simpler example for the time being.

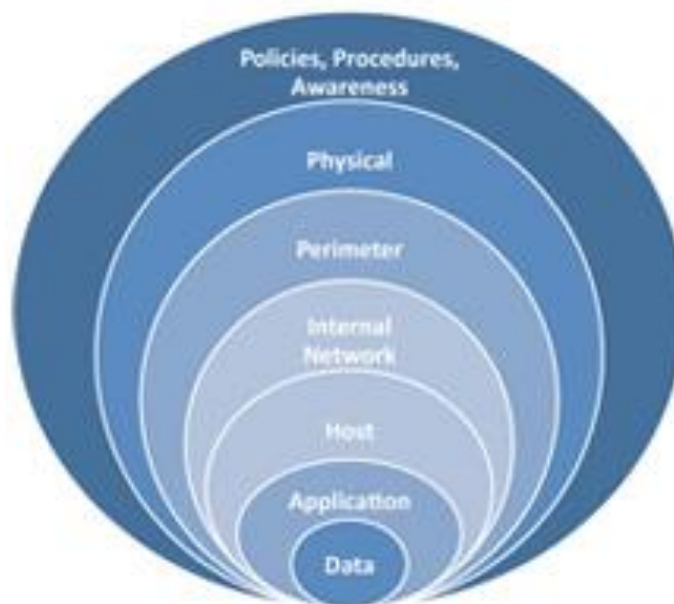


Figure 44: layers of Defense in Depth

As we can see in Figure 45 below, some of the defenses we might use for each of the layers we discussed are listed. In some cases, we see a defensive measure listed in multiple layers, as it applies in more than one area. A good example of this is penetration testing. Penetration testing is a method of finding gaps in our Defenses in Each Layer security by using some of the same

methods an attacker would use in order to break in and is a tactic we might want to use at all layers of our defense. As we move through the course, we will discuss each of these areas in greater detail, and the specific defenses we might want to use for each.

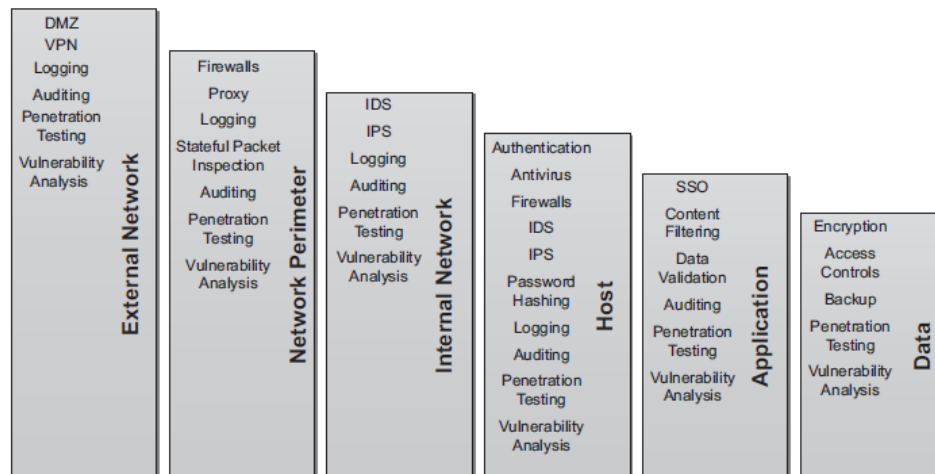


Figure 45: Defense in each layer

## 1.10 INFORMATION SECURITY IN THE REAL WORLD

The concepts we discussed in this chapter are foundational to information security and are used on a regular basis in the course of normal information security tasks in many organizations. We will often find that security incidents are described in terms of their effects, such as breaches of confidentiality, or the authenticity of a given e mail message. Information security is a daily concern for organizations of any size, particularly those that handle any type of personal information, financial data, health care data, educational data, or other types of data that are regulated by the laws of the country in which they operate. In the case of an organization that does not take the time to properly put itself on a good footing as relates to information security, the repercussions can be severe in the sense of reputational Impact, fines, lawsuits, or even the inability to continue conducting business if critical data is irretrievably lost. In short, information security is a key component of the modern business world.

### 1.11 SUMMARY

Information security is a vital component to the era in which data regarding countless individuals and organizations is stored in a variety of computer systems, often not under our direct control. When discussing information security in a general sense, it is important to remember that security and productivity are often diametrically opposing concepts, and that being able to point out exactly when we are secure is a difficult task. When discussing information security issues or situations, it is helpful to have a model by which to do so. Two potential models are the CIA triad, composed of confidentiality, integrity, and availability, and the Parkerian hexad,

composed of confidentiality, integrity, availability, possession or control, authenticity, and utility.

When we look at the threats we might face, it is important to understand the concept of risk. We only face risk from an attack when a threat is present and we have a vulnerability which that particular threat can exploit. In order to mitigate risk we use three main types of controls: physical, logical and administrative.

Defense in depth is a particularly important concept in the world of information security. To build defensive measures using this concept we put in place multiple layers of defense, each giving us an additional layer of protection. The idea behind defense in depth is not to keep an attacker out permanently but to delay him long enough to alert us to the attack and to allow us to mount a more active defense.

## 1.12 CHECK YOUR PROGRES

- 1 PII stands for \_\_\_\_\_.
- 2 \_\_\_\_\_ is defined as protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction.
- 3 A set of security goals, identified as a result of a \_\_\_\_\_, should be revised periodically to ensure its adequacy and conformance with the evolving environment.
- 4 \_\_\_\_\_ is the act of ensuring that data is not lost when critical issues arise.
- 5 HIPPA stands for \_\_\_\_\_.
- 6 CIA stands for confidentiality, integrity, and \_\_\_\_\_.
- 7 In information security, \_\_\_\_\_ is the property, that information is not made available or disclosed to unauthorized individuals, entities, or processes.
- 8 \_\_\_\_\_ refers to the ability to prevent our data from being changed in an unauthorized or undesirable manner.
- 9 Loss of \_\_\_\_\_ can refer to a wide variety of breaks anywhere in the chain that allows us access to our data.
- 10 \_\_\_\_\_ or control refers to the physical disposition of the media on which the data is stored.
- 11 \_\_\_\_\_ refers to how useful the data is to us.
- 12 \_\_\_\_\_ attacks allow unauthorized users to access our data, applications, or environments, and are primarily an attack against confidentiality.
- 13 \_\_\_\_\_ attacks cause our assets to become unusable or unavailable for our use, on a temporary or permanent basis.
- 14 \_\_\_\_\_ attacks involve generating data, processes, communications, or other similar activities with a system.



### ***1.13 ANSWERS TO CHECK YOUR PROGRES***

- 1 Personally Identifiable Information
- 2 Information security
- 3 threat analysis
- 4 Information assurance
- 5 Health Insurance Portability and Accountability Act
- 6 availability
- 7 confidentiality
- 8 Integrity
- 9 Availability
- 10 Possession
- 11 Utility
- 12 Interception
- 13 Interruption
- 14 Fabrication

### ***1.14 MODEL QUESTIONS***

1. Explain the difference between vulnerability and a threat.
2. List six items that might be considered logical controls.
3. What term might we use to describe the usefulness of data?
4. Which category of attack is an attack against confidentiality?
5. How do we know at what point we can consider our environment to be secure?
6. Using the concept of defense in depth, what layers might we use to secure ourselves against someone removing confidential data from our office on a USB flash drive?
7. Based on the Parkerian hexad, what principles are affected if we lose a shipment of encrypted backup tapes that contain personal and payment information for our customers?
8. 8. If the Web servers in our environment are based on Microsoft's Internet Information Server (IIS) and a new worm is discovered that attacks Apache Web servers, what do we not have?
9. If we develop a new policy for our environment that requires us to use complex and automatically generated passwords that are unique to each system and are a minimum of 30 characters in length, such as !Hs4(jOqO\$&zn1%2SK38cnAfKs620!, what will be adversely impacted?
10. Considering the CIA triad and the Parkerian hexad, what are the advantages and disadvantages of each model?

## UNIT II: INFORMATION SECURITY MANAGEMENT SYSTEMS

### 2.1 LEARNING OBJECTIVES

By the end of this unit you should have developed an understanding of:

- How you select appropriate techniques to tackle and solve problems in the discipline of information security management;
- Why security and its management are important for any modern organisation;
- How an information security management system should be planned, documented, implemented and improved, according to the BSI standard on information security management.

### 2.2 INTRODUCTION

Information security<sup>71</sup> underpins the commercial viability and profitability of enterprises of all sizes and the effectiveness of public sector organisations. This unit begins by explaining why information security and its management are important for any modern organisation. This course unit, starts by examining the value that can be placed on information as an organizational asset. The protection of information assets is the subject of the BSI standard, UK on information security management (which is an accepted standard worldwide), and the goes on to explain how an information security management system should be planned, documented, implemented and improved, according to the standard.

### 2.3 WHY IS INFORMATION SECURITY IMPORTANT?

This course introduces you to information security and its management. A succinct definition of *information security* might run as follows: Information security is the collection of technologies, standards, policies and management practices that are applied to information to keep it secure. But why is it important to secure information? And how should its security be managed? To start thinking about these questions, consider the following statements about *information*:

- a. In today's high technology environment, organizations are becoming more and more dependent on their information systems. The public is increasingly concerned about the proper use of information, particularly personal data. The threats to information systems from criminals and terrorists are increasing. Many organisations will identify information as an area of their operation that needs to be protected as part of their system of internal control. (Nigel Turnbull, 2003, p. xi)

---

<sup>71</sup> <http://www.open.edu/openlearn/science-maths-technology/computing-and-ict/introduction-information-security/content-section-1>

- b. Competitive advantage ... is dependent on superior access to information. **(Robert M Grant, 2000, p. 186)**
- c. Information is the oxygen of the modern age. It seeps through the walls topped by barbed wire, it wafts across the electrified borders. **(Ronald Reagan, 1989)**

It is vital to be worried about information security because much of the value of a business is concentrated in the value of its information. Information is, as Grant says, the basis of competitive advantage. And in the not-for-profit sector, with increased public awareness of identity theft and the power of information, it is also, as Turnbull claims, the area of an organization's operations that most needs control. Without information, neither businesses nor the not-for-profit sector could function. Valuing and protecting information are crucial tasks for the modern organisation. If information were easy to value and protect, however, you would be able to buy off-the-shelf information security management solutions. There are three characteristics of information security that make this impossible.

1. The collection of influences to which each organisation is exposed varies with the organisation: the information technology that it uses, its personnel, the area in which it does business, its physical location – all these have an effect on information security.
2. Information security affects every structural and behavioral aspect of an organisation: a gap in a security fence can permit information to be stolen; a virally infected computer connected to an organization's network can destroy information; a cup of coffee spilt on a computer keyboard can prevent access to information.
3. Each individual that interacts with an organisation in any way – from the potential customer browsing the website, to the managing director; from the malicious hacker, to the information security manager – will make his or her own positive or negative contribution to the information security of the organisation.

Thus information security and its management need to be examined within an organizational context. To this end, a major aim of this unit is to give you the opportunity to:

- investigate your organisation and determine the precise mix of information security issues that affect it;
- explain the links between areas of an organisation and navigate your organization's information security web;
- Identify the security contributions of each individual, and so suggest strategies to make the sum of the positive contributions greater than the sum of the negative ones.

## ***2.4 INFORMATION, INFORMATION SECURITY AND INFORMATION SECURITY MANAGEMENT***

### **2.4.1 What is information?**

*Information* comprises the meanings and interpretations that people place upon facts, or data. The value of information springs from the ways it is interpreted and applied to make products, to provide services, and so on. Many modern writers look at organisations in terms of the use they make of information. For instance, one particularly successful model of business is based on the assets that a firm owns. Assets have traditionally meant tangible things like money, property, plant, systems; but business analysts have increasingly recognised that information is itself an asset, crucial to adding value. As brought out earlier, information underpins competitive advantage. Indeed, there are writers, such as Itami and Roehl (1987), who believe that the true value of an organisation is in the information it uses and creates. But, of course, there is a negative side too: the use of information in both the for-profit and not-for-profit sectors is increasingly the subject of legislation and regulation, in recognition of the damage its misuse can have on individuals.

### **2.4.2 What is information security?**

Seen in the way we have just defined it, information is a valuable asset. *Information security* protects information (and the facilities and systems that store, use and transmit it) from a wide range of threats, in order to preserve its value to an organisation. This definition of information security is adapted from that of the American National Security Telecommunications and Information Systems Security Committee (NSTISSC). There are two important characteristics of information that determine its value to an organisation:

- the *scarcity* of the information outside the organisation;
- the *shareability* of the information within the organisation, or some part of it.

Simplifying somewhat, these characteristics state that information is only valuable if it provides advantage or utility to those who have it, compared with those who don't. Thus the value of any piece of information relates to its levels of shareability and scarcity. The aim of information security is to preserve the value of information by ensuring that these levels are correctly identified and preserved. Threats to information influence the organisation's ability to share it within, or to preserve its scarcity outside. And threats that are carried out can cost millions in compensation and reputation, and may even jeopardize an institution's ability to survive. Here are some examples in which the making available of information that should have been kept scarce or the restricting of information that should have been shareable has damaged an organisation.

#### **Example 1: Softbank – theft of consumer data for extortion**

Softbank of Japan offers broadband internet services across Japan through two subsidiaries – Yahoo! BB and Softbank BB. In February 2004, the bank announced that the security of 4.5 million customer records had been compromised: data from both subsidiaries had been illegally

copied and disseminated. The leaked details included customer names, home phone numbers, addresses and email IDs, but did not include passwords, access logs or credit card details. Softbank became aware of the problem only when they were approached by two groups of extortionists. The criminals produced apparently genuine customer data and threatened that all of the data would be posted to the internet if they were not paid a large sum of money.

Japanese police made three arrests but suspected that there may have been connections to organized crime and the political far-right. Amazingly, the police concluded that there had in fact been two simultaneous, yet independent, extortion attempts against Softbank, both of them masterminded by employees of the company. All of the people accused of extortion had been authorized to access the customer data; but it appeared that Softbank had inadequate procedures to protect against its unwarranted copying and dissemination.

The bank immediately announced a tightening of security, further restricting access to their systems and enforcing tighter security on all of their subsidiaries. Profuse apologies were offered to the affected customers and ¥4 billion (£20 million) were paid in compensation. Furthermore, Softbank BB's president, Masayoshi Son, announced that he and other senior executives would take a 50 per cent pay cut for the next six months.

In this example, the threat was to reduce the value of an organisation by revealing information that should have been a well-kept secret – scarce-within as well as scarce-without. It cost the company £20 million in compensation and affected its reputation.

### **Example 2: UCSF Medical Center**

In October 2002, the University of California, San Francisco (UCSF) Medical Center received an email message from someone who claimed to be a doctor working in Pakistan and who threatened to release patient records onto the internet unless money owing to her was paid. Several confidential medical transcripts were attached to the email. UCSF staff were mystified; they had no dealings in Pakistan and certainly did not employ the person who sent the email. The Medical Center began an immediate investigation, concentrating on their transcription service, which had been outsourced to Transcription Stat, based in nearby Sausalito. It transpired that Transcription Stat farmed out work to some fifteen subcontractors scattered across America. One of these subcontractors was Florida-based Sonya Newburn, who in turn employed further subcontractors, including one Tom Spires of Texas. No one at Transcription Stat realized that Spires also employed his own subcontractors, including the sender of the email. The sender alleged that Spires owed her money, and had not paid her for some time.

Newburn eventually agreed to pay the \$500 that the email sender claimed was owed to her. In return the sender informed UCSF that she had had no intention of publicizing personal

information and had destroyed any records in her care. Of course, there is no way to prove that the records have actually been destroyed.

Naturally, you would not wish your own medical records to be publicised: they should be scarce. This threat cost the organisation little in money terms, but how much in reputation? Just what is a reputation worth? Or, to put it another way, how much is it worth paying in information security to protect a reputation?

### **Example 3: Logic bombs**

In May 2000, Timothy Lloyd was found guilty of causing between \$10 million and \$12 million worth of damage to Omega Engineering, an American company specializing in precision engineering for clients, including the US Navy and NASA. Lloyd had been employed with Omega for 11 years, rising to the post of system administrator, and was responsible not only for the day-to-day operation of the company's computers but also for their disaster-recovery process. In 1996, Lloyd became aware that he was about to be sacked and wrote a logic bomb – a six-line destructive program – which he installed on Omega's servers. Ten days later, Lloyd was dismissed and his logic bomb exploded, destroying company contracts and proprietary software used by Omega's manufacturing tools. Although Omega had instituted a backup procedure, Lloyd's account privileges had allowed him to disable these recovery systems. The damage done by his logic bomb was permanent.

When the logic bomb ‘exploded’ it wiped out information that was needed for the company to operate. As a result of lost business, Omega was forced to lay off some 80 employees and found itself rewriting the very software which had once given it a competitive edge over its rivals. In effect, what Lloyd managed to do, in the most decisive way possible, was to prevent vital information being shared.

### **2.4.3 What is information security management?**

*Information security management* is the process by which the value of each of an organisation's information assets is assessed and, if appropriate, protected on an ongoing basis. The information an organisation holds will be stored, used and transmitted using various media, some of which will be tangible – paper, for example – and some intangible – such as the ideas in employees' minds. Preserving the value of information is mainly a question of protecting the media in which it is contained.

Building an information security management system (as we present it in this course) is achieved through the systematic assessment of the systems, technologies and media used for information assets, the appraisal of the costs of security breaches, and the development and deployment of countermeasures to threats. Put simply, information security management recognizes the most vulnerable spots in an organisation and builds armor plating to protect them. The diversity of the media used for an organization's information assets is just one of the difficulties to be overcome in building an information security management system. Among other difficulties are the following.

- Effective information security measures often run counter to the mission of an organisation. For instance, the safest way to secure a computer and the information on it is to allow no access to it at all!
- The requirement to respect the needs of the users of the organization's information, so that they can continue to do their jobs properly.

We can deduce that no single solution can address all possible security concerns. The only strategy is to engineer a fit-for-purpose solution that achieves a suitable balance between risks and protection against them. As with all management systems, the engineering of a fit-for-purpose information security management system is achieved through hard work. Part of the hard work is, of course, an understanding of the technologies involved– we provide the necessary details in this course. Other major tasks are identifying the needs of the different stakeholders and ensuring coverage of every procedure and policy that involves the development, transformation or dissemination of sensitive information.

**Thus, information security management is a development activity analogous to the development of software, and we shall present in this way throughout this course.**

## ***2.5 INFORMATION SECURITY IMPERATIVES AND INCENTIVES***

The design of a successful information security policy and strategy for any organisation requires an assessment of a number of key factors. These factors can be categorized as either *imperatives* or *incentives*. Imperatives are pressures that force you to act. Incentives are the rewards and opportunities that arise from acting. We will examine the main imperatives confronting organisations in the proceeding sections. These arise either from threats to information assets or from the obligation to comply with existing law , with codes governing the management and control of public and private assets and the protection of the interests of stakeholders. We place all of these imperatives in a wider framework of ethical practice in information management. We will also look briefly at some of the incentives for engaging in information security management. Incentives mainly come in the form of opportunities to reduce the cost of existing ways of working and new options for pursuing an organization's objectives.

### **2.5.1 Imperatives**

Imperatives generally arise from three sources:

- **threats:** companies that depend on information and the technologies that carry it have to protect these resources from a wide range of threats;
- **legislation:** many countries have enacted legislation to govern the storage and use of information;
- **regulation:** many countries have regulations governing the management and control of public and private assets.

## 2.5.2 Incentives

We identified the following benefits for the Organisation, treating information security seriously

- As an organisation, it must meet stakeholders' expectations of continuity, confidentiality and privacy of information. Taking information security seriously helps the organisation fulfill its obligations to its wider community.
- If the organisation can demonstrate that it takes information security seriously, this may help it to foster functional and commercial relationships with other organisations that give priority to information security. For instance, in research relationships with commercial organisations, our organisation would be given access to commercially sensitive information, such as business rules, critical systems, etc. The ability of the organisation to take information security seriously means that such partnerships are easier to establish, and will endure.

## 2.6 INFORMATION ASSETS

In the previous section, explained that information is an important asset to an organisation. In this section you will study, in some detail, the characteristics of information assets that make them valuable, and so worth protecting. In recent years, a combination of computerized processing systems and electronic communication technologies has made possible new forms of working and trading based on the electronic exchange of information. Such activity is called *e-business* or *e-commerce*. Two new, but already familiar, models of organisations working together electronically in this way are the following:

- **Business-to-business (b2b) commerce**, in which businesses work closely together, using the internet, to trade information, services and/or products. Examples include financial management and Web-server management.
- **Business-to-customer (b2c) commerce**, in which the internet is used to connect a business directly to the customer without the need for premises such as shops or warehouses. Examples include many small software firms, the book retailer Amazon and economy airlines.

Despite their names, these models apply to not-for-profit as well as for-profit organisations. For example, an academic institution makes use of the b2c model. The OASIS Universal Description, Discovery and Integration (UDDI) protocol is a directory service that enables organisations and applications to find and use Web services over the internet. The supporting website (<http://uddi.xml.org>) has an interesting collection of white papers on the technologies involved and their use.

Of course, the electronic exchange of information takes place within individual organisations as well as between them, typically reducing communication delays. For example, separate business units within a company use email to transfer documents almost instantly, whereas in the past



they had to rely on a comparatively slow internal mail system. Highly efficient intra-organizational workflows are now possible through electronic communication.

However, these new forms of communication and commerce also present new dangers since they make an organization's information assets subject to new threats. Access to vital assets may no longer be restricted to those who have a key for the lock of the door that protects a building. Electronic communication may make the whole world your market place; but there is a danger that it will also make the whole world your premises.

In following sections we shall examine the characteristics of information assets that make them worth protecting. We shall also discuss the concepts of shareability, scarcity, confidentiality, integrity and availability in relation to these assets.

### **2.6.1 Information in an e-business age**

Sharing information in business is itself a risky business. The information that is exchanged between b2b partners, for instance, may include order information, customer details and strategic documents. Such information could be priceless to outsiders. As you saw in the previous section, huge costs can result from information getting into the wrong hands.

In sharing information, an organisation also needs to be aware of the various laws, regulatory frameworks and codes of practice. Failure to comply with these can lead to disciplinary action against individuals and to legal action against organisations. In such situations, directors and managers are duty bound to be cautious and vigilant.

But the rewards of the e-business age can be immense: information has become a powerful source of competitive advantage, and may contribute massively to the value of an organisation and to its ability to meet its mission. And this is not just theory. One only needs to look at the difference between the *book value* of an organisation – the value placed on it by accountants – and its *market value* – the value placed on it by investors – to see the significance of information. For instance, in 1997 Coca-Cola had a market value of \$33.4 billion, whereas its book value was only just above \$1.2 billion: intangible assets, including information, contributed to over \$30 billion of additional value. In the same year, Microsoft had a market valuation 21.4 times its book value: intangible assets, such as information, expertise and the company's huge customer base, made up the difference.

### **2.6.2 Scarcity and Shareability**

Modern business theory now views an organization's intangible, rather than its tangible, assets as the reservoir of much of its value. Even a not-for-profit organisation requires information to be shared and protected for its mission to be accomplished. With this new perspective has come a re-evaluation of the methods to be used to protect the value of an organisation. Historically, four walls were all that was needed to demarcate the inside of an organisation from the outside; and

four sturdy walls were all the protection necessary for complete safety. Today, it is those with whom the organisation shares information, and those from whom it keeps it secret, that determine organizational boundaries.

The existence of such organizational boundaries led Grant (1998) to the following observations concerning assets (in the most general sense):

- assets should be *shareable* (i.e. available for use) within the organisation, or some part of it;
- **assets** should be *scarce* (i.e. not available for use) outside the organisation.

Grant goes on to assert that, in for-profit organisations, the combination of shareability and scarcity is the basis of competitive advantage. In not-for-profit organisations, shareability of information contributes to the discharge of the organisation's mission, and its scarcity is often required by law or by other codes.

We can elaborate Grant's argument. Any information asset has two regions associated with it. First, it has a *shareability region* that contains all the systems and people to which and to whom the information asset should be available. Second, it has a *scarcity region*, containing *all other* systems and people.

To maximize an information asset's utility (and thus its value) to an organisation, it should be available within its shareability region whenever needed: if such an asset is not available when some authorized person or system requests it, then this is a failure of shareability. You will have experienced such failures yourselves: not having access to your email when you need it, for example, or not being able to remember your password for some machine or system. In a wider context, an inaccessible customer or product database may have a serious impact on an organization's ability to carry out its mission.

Moreover, for it to be useful to an organisation, an information asset should always be *correct* within its shareability region: if it becomes corrupted or damaged in some way it will be less useful, or even worthless. For example, you undoubtedly have had personal experience of word-processed documents that are unopenable, or can be accessed but have been corrupted in some way.

An information asset should either be unavailable in its scarcity region or, if needs dictate that it must be available, it should be damaged or disabled in some way to remove its value as far as the organisation that owns it is concerned. Examples of information that has to be released into its scarcity region are easy to find in the commercial world, especially on the internet. *Demoware*, for instance, is commercial software that has had some important function disabled, so that it can be freely distributed for demonstration purposes while ensuring that anyone who finds it useful has to pay a license fee for the complete version.

### 2.6.3 Confidentiality, integrity and availability

To preserve the value of an information asset, an organisation needs to sustain simultaneously its scarcity and its shareability within their respective regions. This is the critical high-level information security goal for any information asset; it is the entire rationale of an information security management system. To maintain the security of an information asset, an organisation must:

- *either* make the information asset unavailable in its scarcity region, i.e. make it **confidential** to the shareability region;
- *or* damage or disable the information asset before allowing it into the scarcity region, i.e. undermine the **integrity** of the asset. The damage or disablement must be such that the original information asset retains most, or all, of its value to the organisation.

At the same time, to ensure that an information asset maintains its value, an organisation must:

- ensure that the information asset is *available* within the shareability region;
- maintain the **integrity** of the information asset within the shareability region.

Most authors accept that confidentiality, integrity and availability are the most important information security requirements— requirements rather than goals, because they can, in principle, be controlled directly by an organisation. Because of this, they form the basis of most modern approaches to information security management, including that of the Indian IT Act, which covers good definitions of all three terms. Information security management is therefore concerned with ensuring an information asset's confidentiality, availability and integrity; and breaches in information security can be defined as a reduction in one or more of these three features. Thus, breaches of an information asset's security requirements have occurred when:

- the confidentiality of the information asset is reduced by it being disclosed outside its shareability region;
- the integrity of the information asset is harmed by it being corrupted or damaged inside its shareability region;
- the integrity of the information asset is preserved after it has crossed from the shareability to the scarcity region;
- the availability of the information asset is reduced inside its shareability region.

In addition, the availability of an information asset can be reduced by:

- the destruction or loss of the information asset, the hardware it resides upon, or the software that interacts with it;
- the interruption, for a period of time, of access to the information asset.

The security requirements of an information asset may change over time, as may its value to an organisation. Consider this simple example relating to the confidentiality of an information asset. Suppose you have information that a company is soon due to make an announcement that will cause its stock price to rise or fall. The fact that one could make a killing on the stock market with such information makes it very valuable, and so subject to the highest levels of confidentiality. However, after the official announcement, the information loses its value, and so the requirement of confidentiality is no longer an issue. *Insider dealing*, which includes the

inappropriate release of such information, is a criminal offence under the Criminal Justice Act 1993. Similarly, time can affect the security requirements regarding availability and integrity: the need for an information asset to be available will be greater at some times than others, as will the need for its integrity.

## ***2.7 PLANNING AN INFORMATION SECURITY MANAGEMENT SYSTEM***

In this section we will discuss the process required by Information Security Management for planning an information security management system (ISMS). We present ISMS development as a process involving four tasks, each of which may be subdivided into stages. This section also examines the managerial and organizational structures that the Standard recommends to support ISMS development and looks in detail at the ISMS documentation task.

### **2.7.1 The Standard's approach to planning an ISMS**

The Standard describes the planning of ISMS, which it refers to as the 'Plan activity', as follows: The Plan activity is designed to ensure that the context and scope for the ISMS have been correctly established, that all information security risks are identified and assessed, and that a plan for the appropriate treatment of these risks is developed. It is important that all stages of the Plan activity are documented for traceability and for the management of change.

This description suggests an approach to the planning and documentation of an ISM that comprises four tasks. These four tasks are not identified explicitly in the Standard. The *documentation* task, which takes place throughout the process, can be summarized as follows.

- *ISMS documentation*, in which the context and scope of the ISMS, and its rules for assessing risk are determined and in which the documentation that makes progress through the stages of the process traceable and the management of change possible is generated.

This task begins at the same time as, runs in parallel with, and records the decisions of the three other tasks, which take place sequentially and concern the *planning* of the ISMS.

- *Asset identification*, in which the information assets that are to be handled by the ISMS are identified, and their security requirements are established.
- *Risk assessment*, in which the risks of breaches of the security requirements of information assets are assessed.
- *Risk treatment*, in which a plan for the management of the risks is developed.

The planning tasks complement and drive the documentation task, by providing the operational details of what the ISMS will do. The relationships between the four tasks are illustrated in Figure below:

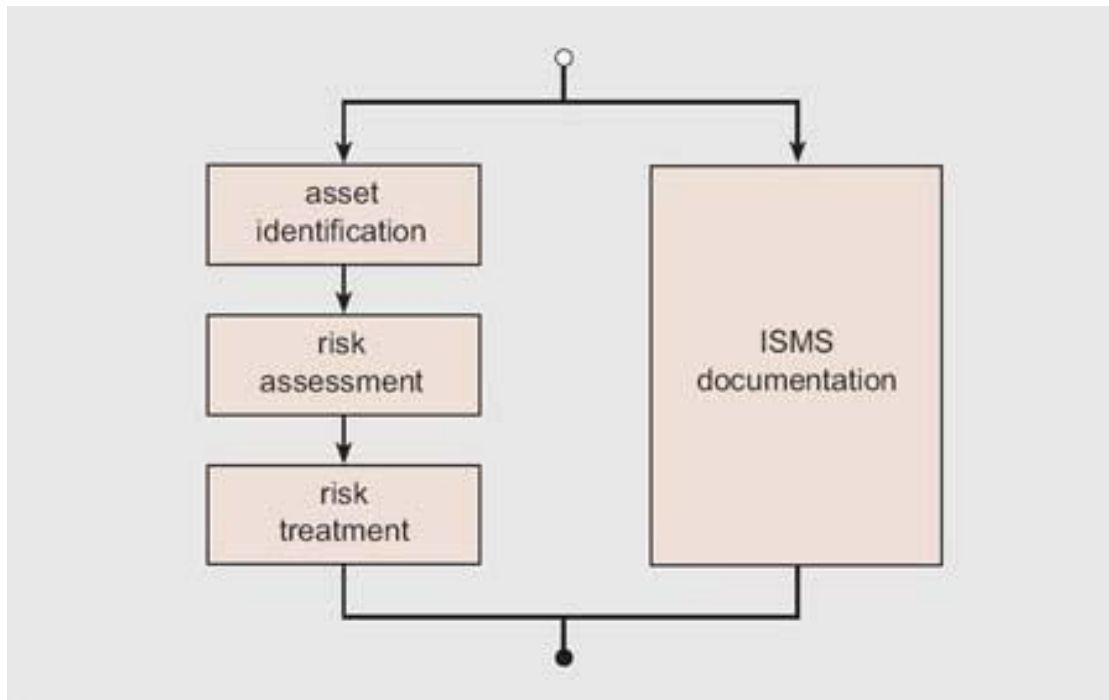


Figure 46: The relationships between the four tasks comprising

The four tasks are subdivided into stages, each of which is described in subsequent sections.

### 2.7.1.1 ISMS documentation

ISMS documentation is carried out at organisation level. Its purpose is to define the scope and context of the proposed system, and the approach to information security management that it will embody. It has five stages: three that initiate the planning process (Stages 1 to 3) and two that complete it (Stages 8 and 9).

- **Stage 1: define the scope of the ISMS:** The context and scope of the ISMS are defined by considering the nature of the organisation, the business (or service) area in which it operates, and its location, assets and technology. The scope of the ISMS is a statement of which information assets are to be protected.
- **Stage 2: define an ISMS policy:** An ISMS policy, often referred to simply as an information security policy, is drawn up. This important document underpins the ISMS and contributes to the traceability and repeatability of its processes. It should, among other things, set up criteria against which security risks to information assets can be evaluated.
- **Stage 3: define a systematic approach to risk assessment:** A document specifying a systematic approach to risk assessment is written. This must include a process for evaluating the likelihood of a risk to an information asset's security requirements, and the impact of a breach of them, along with a definition of what constitutes acceptable risk.
- **Stage 8: prepare a Statement of Applicability:** The Statement of Applicability of the ISMS is completed, based on information gathered at Stage 7 (during risk treatment).

- **Stage 9: obtain management approval:** The complete ISMS documentation, consisting of the papers drawn up in Stages 1, 2, 3 and 8, is submitted to senior management for approval.

### 2.7.1.2 Asset identification

The asset identification task is carried out at unit level within an organisation, in light of organisation-wide policies set out in Stages 1 to 3. It uses Stage 1's description of the scope of the ISMS to determine the information assets that are to be protected.

- **Stage 4.1: identify the assets at risk:** The information assets at risk are identified, along with their owners, their locations, their values and their information security requirements. The results are documented.

### 2.7.1.3 Risk assessment

The risk assessment task is also carried out at unit level, in light of policies set out in Stages 1 to 3 and for the assets identified in Stage 4.1.

- **Stages 4.2, 4.3 and 4.4:** identify the risks
- **Stage 4.2:** determines systematically the possible threats to the assets identified in the asset identification part of the process.
- **Stage 4.3:** identifies vulnerabilities that might allow those threats to become successful attacks on the assets.
- **Stage 4.4 :** uses the evaluation mechanisms established in Stage 3 to assess the impact of breaches of the assets' security requirements.
- **Stage 5: assess the risks:** The risks to information assets are assessed using the risk assessment strategy determined in Stage 3. Each breach of security is assigned a level of risk determined by its likelihood and by its impact on the organisation.
- **Stage 6: identify and evaluate options for the treatment of risks :** The risks have their treatment chosen. The choices are to: accept the risk; avoid the risk; transfer the risk; control the risk. A risk is accepted only if it meets the criteria for risk acceptance defined at Stage 3. If the choice is to avoid a risk or transfer a risk (to another organisation, such as an insurer or subcontractor), a suitable means of avoidance or transfer is identified. Otherwise the choice is to control (i.e. lower) the risk to the asset (by taking measures to reduce the asset's vulnerabilities), in which case the risk is assigned a priority level for treatment.

Documents generated in the risk assessment task must present evidence that every risk has been assessed, along with a justification for the outcome – acceptance, avoidance, transfer or control – of each individual assessment.

### 2.7.1.4 Risk treatment

The risk treatment task is again carried out at unit level, in light of policies set out in Stages 1 to 3. The risks treated are those chosen for control at Stage 6.

- **Stage 7: select control objectives and controls:** For each risk chosen for control at Stage 6, a suitable control (countermeasure) must be selected from those suggested in the

Standard or from elsewhere. The risks are treated in order of priority, according to the priority levels assigned at Stage 6.

Suitable controls are listed in Annexure A to Part 2 of the Standard, though this list is not exhaustive.

Documents drawn up in the risk treatment task should include evidence that each risk has been treated appropriately.

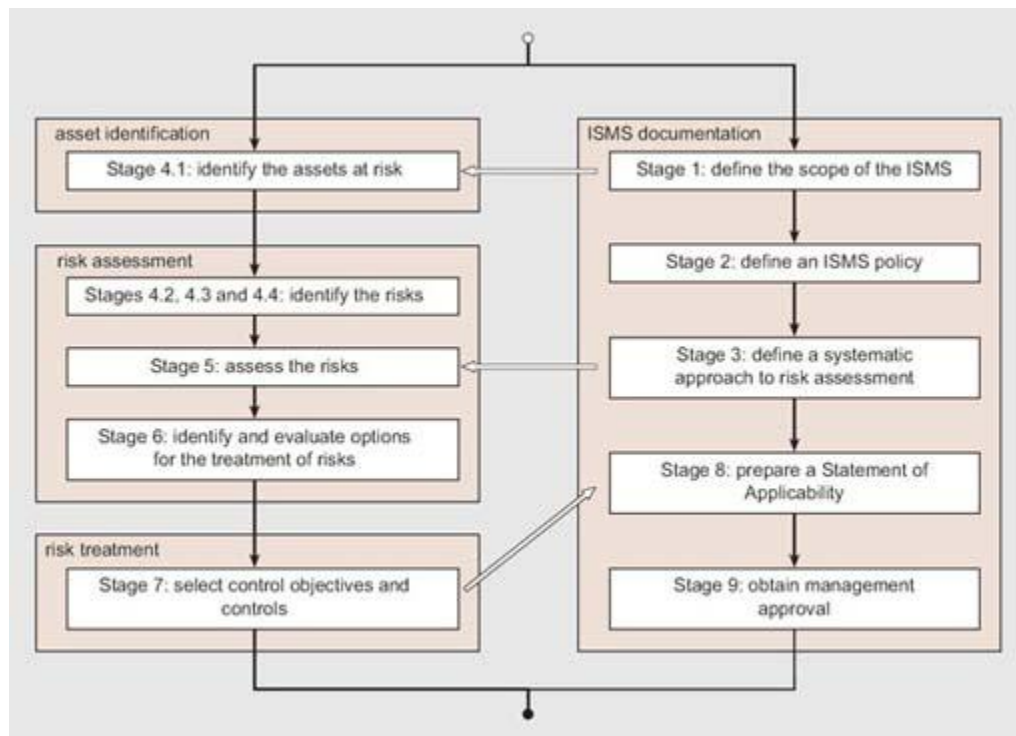


Figure 47 : The relationship between the stages and the tasks

## 2.8 OTHER APPROACHES TO INFORMATION SECURITY MANAGEMENT

Many of the approaches to planning an ISMS to be found in the literature follow a three-phase, rather than a four-task, approach. For instance, Moses (1994) stipulates seven steps in three phases:

- **Initiation:** the identification of information assets and their security requirements;
- **Analysis:** the identification of possible risks to the security requirements of information assets, of the vulnerabilities to those risks, and of the impact on the organisation of breaches of the security requirements;
- **Management:** the identification and justification of countermeasures where needed.

Moses's initiation phase corresponds to our asset identification and his analysis and management phases together correspond to our risk assessment and treatment.

Alberts and Dorofee (2003) specify another three-phase process. Again, the task of the first phase is to identify the organization's information assets and their security requirements, but it also includes a threat analysis. In Alberts and Dorofee's second phase, the technology systems with which each information asset is associated are determined, so that vulnerabilities to the threats uncovered in the previous phase can be listed and assessed. Each system is then evaluated for the probability and impact of an attack, so that threats and risks can be prioritized. In the third and final phase, the plan comes together with the choice and tailoring of controls.

You will notice that the three-phase approaches of Moses and of Alberts and Dorofee omit the ISMS documentation task. Moreover, neither of these approaches covers the preparation of a Statement of Applicability or the submission of the final set of documents to senior managers for approval. The difference is that, in both cases, the authors focus only on risk analysis and management, and so miss the Standard's requirement for certification of the ISMS. The documents generated in the ISMS documentation task are a major component of what would be delivered to a certifying authority, and provide much of the basis for traceability and for the management of change.

## **2.9 SETTING UP AN ISMS**

Clause 4.1 of Part 1 of the British Standard describes the processes and personnel required to support an ISMS under development or in operation. Chapter 4 of *IT Governance: A Manager's Guide to Data Security & BS 7799/ISO 17799* provides a detailed description of each of the components of such support systems, as well as exploring their interrelationships.

## **2.10 ISMS DOCUMENTATION**

In this subsection we shall consider Stages 1, 2 and 8 of the ISMS documentation task. Stage 3 is considered in Section 6. We shall not discuss Stage 9 in this course.

### **2.10.1 Context, scope and information security policy**

An ISMS is defined in Clause 3.4 of Part 2 of the British Standard as a management system, based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve information security. Some organisations will want to protect all of their information assets. Others, depending on the business risks and other hazards they face, may want to consider an ISMS that protects only some of them. Examples of organizational units that might need protecting include research and development, payroll, databases and – given their increasing importance and vulnerability – any online operations.

As you have seen, this decision on which areas to protect – the question of context and scope – launches the ISMS planning process. By defining the *scope* of the ISMS – which parts of the organisation need its protection – the information assets that need protecting begin to become visible. Defining the *context* of the ISMS – the relationship (business, physical, legal, regulatory, etc.) the protected areas hold to the remainder of the organisation and to the rest of the world – sheds light on the threats that they must be protected against.



The definitions of the scope and context of the ISMS are recorded in the information security policy.

### **2.10.2 The Statement of Applicability**

The composition of the Statement of Applicability of the ISMS is Stage 8 of the ISMS planning process.

## **2.11 RISK ASSESSMENT AND ASSET IDENTIFICATION**

We have already discussed the ISMS planning and documentation process in general and also went into the details of Stages 1, 2 and 8 of the ISMS documentation task. In this section, we shall discuss Stage 3 of the ISMS documentation task and see how to define a systematic approach to risk assessment. We shall also look at the asset identification task. The remaining two tasks, risk assessment and risk treatment, are outside the scope of this course.

### **2.11.1 A systematic approach to risk assessment**

In the previous sections of this course you learned of the immense value of information to modern organisations. However, without a storage medium of some kind – paper, a hard disk, a white board, a human memory – information is entirely ephemeral. Once recorded in a medium, though, information endures and can be manipulated; but it also becomes subject to the vulnerabilities of that medium and of the systems that access that medium. And once there are vulnerabilities, there are threats to the security of the information.

In this subsection, we look at how we can develop a systematic approach to assessing the risk of different threats to the security of information assets by analysing the vulnerabilities of the media and systems used to store and manipulate the assets and by estimating the likelihoods of the threats. We shall see how this information can be combined with an evaluation of the impact on an organisation of each security breach to provide a risk assessment for each threat to an information asset.

#### **2.11.1.1 Threats, outcomes and impacts**

For the purposes of this course, we define a *threat* to an information asset as a possible way in which the asset can have its security requirements breached, and we define the *outcome* of a threat as the way in which the asset's security requirements would be breached if the threatened action were to occur. Recall from Section 4 that the security requirements are confidentiality, integrity and availability.

A complete picture of the relationship between an information asset, the threats to it and their outcomes is set out in Figure 48. Figure 48 is adapted from Figure 5-4 of Alberts and Dorofee (2003).

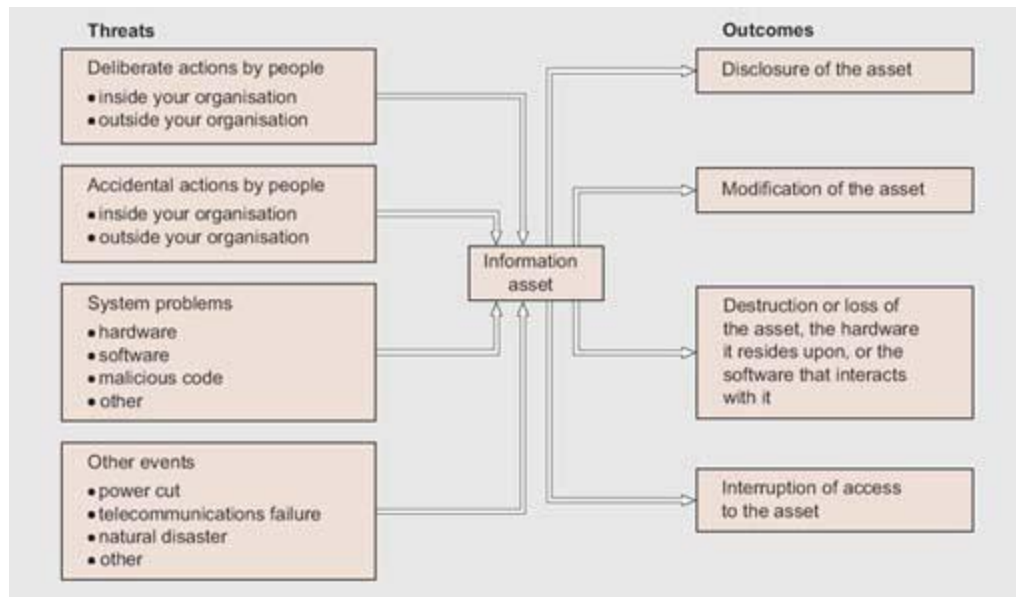


Figure 48 : The relationship between an information asset, the threats to it and their outcomes<sup>72</sup>

Figure 48 classifies the threats into four types, as follows.

- **Deliberate actions by people**, which can come from two groups of persons: those *inside* an organisation and those *outside* it. Examples include a malcontent employee shredding important documents and a hacker attacking a password file. The threats from deliberate actions by people can be further classified into malicious and non-malicious threats.
- **Accidental actions by people**, which again can come from the same two groups: those *inside* and those *outside* an organisation. Examples might be an employee accidentally deleting an important file and a family member spilling coffee on the keyboard of a computer.
- **System problems**, which include: hardware problems (for example, a server crash making the files on a hard disk unrecoverable); software problems (such as bugs, or the system clock being incorrect and causing a backup program to function incorrectly); and malicious code (maybe a virus or Trojan horse).
- **Other events** include power cuts, telecommunications failures, fire, rodents, meteorites, earthquakes, volcanic eruptions, cosmic rays, and so on. Even severe weather conditions can be a threat to some equipment.

The figure also identifies four possible outcomes for each threat, as follows.

- **Disclosure of the asset**, such as when a hacker releases an online trader's customers' credit card details. In this case, the outcome of the threat is a breach of an information asset's confidentiality requirements.
- **Modification of the asset**, such as a fraudulent increase in the balance of a bank account. Here, the outcome is a breach of an information asset's integrity requirements.
- **Destruction or loss of the asset, the hardware it resides upon, or the software that interacts with it**, such as the loss of an important file due to scratched optical backup

<sup>72</sup> [http://www.open.edu/openlearn/ocw/mod/oucontent/view.php?id=2826&extra=thumbnail\\_idp7881152](http://www.open.edu/openlearn/ocw/mod/oucontent/view.php?id=2826&extra=thumbnail_idp7881152)

media. In this case the outcome is a breach of an information asset's long-term availability requirements.

- **Interruption of access to the asset**, such as a web-server upgrade interrupting online access to an organization's web services. Here the outcome is a breach of an information asset's short-term availability requirements.

Related to the concept of threat is that of *attack*: a threat is a *way* of breaching the security requirements of an information asset; an attack is an *attempt* to breach them. Any threat could turn into an attack, which could be successful or unsuccessful. An unsuccessful attack has no impact.

The *impact* on an organisation of a successful attack on an information asset will depend on how, and to what degree, the organization's operations are disrupted. For instance, the impact could be measured in terms of: the embarrassment caused to the organisation, or its loss of reputation; the harm caused by its being unable to fulfill its mission; lost revenue, wasted investment, or other financial loss; or legal or regulatory liabilities incurred. The relationship between threat and impact is a simple one: a *threat* has the potential to have an *impact* on an organisation.

### 2.11.1.2 Threats and vulnerabilities

A hacker who threatens your organization's information assets is taking advantage of vulnerabilities in the media and systems which handle them. Vulnerabilities and threats clearly go hand-in-hand: each threat is directed at a vulnerability.

The relationship between information assets, threats, vulnerabilities and existing defences is illustrated in Figure 49, which depicts an information asset that is only partially protected by the defences of the media and systems handling it. Some threats will be defeated by these defences, but other threats can take advantage of unprotected vulnerabilities and, in the worst case, compromise the information asset. The aim of an ISMS must be to identify and repair crucial vulnerabilities in media and systems. Figure 49 is adapted from a figure used in a course presented at Stevens Institute of Technology in 2003.

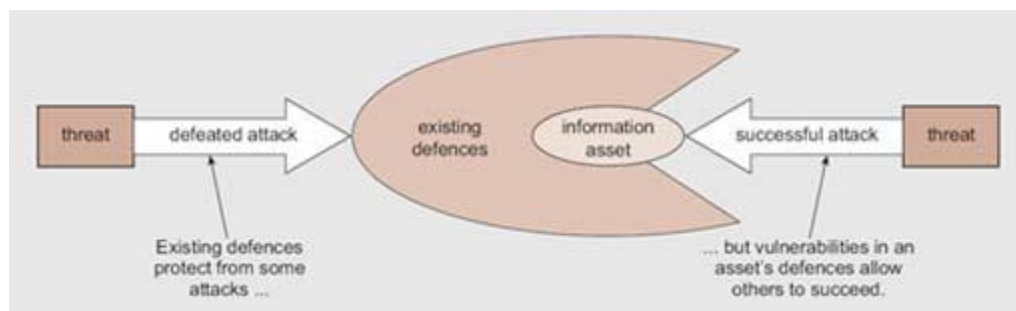


Figure 49: The relationship between information assets, threats, vulnerabilities

### 2.11.1.3 Likelihood, impact and risk

Having looked at threats, vulnerabilities, outcomes and impacts, we are now in a position to offer a definition of risk with regard to threats to the information assets of an organisation. This definition will lead to an approach to measuring and assessing risk that is consistent with the Standard and with *IT Governance: A Manager's Guide to Data Security & BS 7799/ISO 177799* (the Set Book). This systematic approach to risk assessment corresponds to Stage 3 of the ISMS documentation task in the ISMS planning process.

Parker (1981, p. 141) defines *risk* as ‘the product of the amount that may be lost [the *impact*] and the probability of losing it [the *likelihood*]’. Parker here uses the word ‘product’ in its loosest mathematical sense, i.e. as the combination of two quantities in some way. According to this definition, then, risk comprises two quantities – an impact and a likelihood – combined in some way. As we have seen, the *impact* of a threat is harm done to an organisation if the threat were to turn into a successful attack. The *likelihood* of the threat is the probability that the threat will result in a successful attack.

Parker's definition of risk suggests that both the impact and the likelihood could be expressed as numbers. However, estimating numerical values for these quantities is, as you might imagine, fraught with difficulty. Therefore, in this course, we take the pragmatic, but effective, widely used and respected, *qualitative* approach to risk, in which impact and likelihood can take only three values: low, medium or high. These values are best interpreted in their relation to one another: for instance, a low-impact event will cost the organisation less than a medium-impact event, and a medium-likelihood event will, on average, occur less frequently than a high-likelihood event. However, the ISMS documentation should include some rough-and-ready definition of what ‘low’, ‘medium’ and ‘high’ are to be taken to mean. For example, definitions of levels of impact might be:

- low impact means ‘has negligible effect on the organisation’;
- medium impact means ‘has considerable effect on the organisation, but the organisation's existence is not threatened’;
- high impact means ‘the organisation's existence is threatened’.

For likelihood, examples are:

- low likelihood means ‘practically never’;
- medium likelihood means ‘in the order of once a year’;
- high likelihood means ‘in the order of once a week, or more often’.

The choice of scales for measuring impact and likelihood should be justified by reference to the organization’s objectives and its environment.

Using these scales, we can combine impact and likelihood to produce a *risk combination table*, which provides a measure of risk. One way of doing this is to consider impact and likelihood as being equally important, giving rise to the following risk combination table.

Table 6 : Risk combination table,

	Low likelihood	Medium likelihood	High likelihood
Low impact	low risk	low risk	medium risk
Medium impact	low risk	medium risk	high risk
High impact	medium risk	high risk	high risk

Using this table, we would classify a medium impact, high likelihood threat as of high risk.

Another possible risk combination table, which de-emphasises impact, is the following.

	Low likelihood	Medium likelihood	High likelihood
Low impact	low risk	low risk	low risk
Medium impact	low risk	medium risk	medium risk
High impact	medium risk	high risk	high risk

Using this table, we would classify a medium impact, high likelihood risk as of medium risk. The final task in defining the organization's approach to risk is to decide what constitutes an acceptable level of risk. If a risk combination table is being used, there are only three possibilities.

1. No risks are acceptable: all risks, whether low, medium or high, should be treated.
2. Low risks are acceptable: only medium and high risks should be treated.
3. Low and medium risks are acceptable: only high risks should be treated.

For any organisation, the choice will be based upon several interrelated factors, including the resources (money, personnel, etc.) available for implementing the ISMS, past experience of information security breaches, and the maturity of the current ISMS (if there is one). It should also reflect the current approach to risk of other organisations in the same sector. In addition, an organization's approach to risk may change if new legislation or regulation comes into force, or if new contractual obligations arise.

The approach to risk – the characterization of impact and likelihood levels, the risk combination table and the acceptable level of risk, together with their justifications – is recorded as part of Stage 3 of the ISMS documentation task in the ISMS planning process.

#### 2.11.1.4 Asset identification

You have now completed your study of the ISMS documentation task in the ISMS planning process. In this subsection we study the asset identification task. You saw in the previous section that asset identification consists solely of Stage 4.1 of the ISMS planning process, in which the information assets at risk are identified, along with their owners, their locations, their values and their information security requirements. This stage can be subdivided into four steps.

- **Step 1:** identify the boundaries of what is to be protected.
- **Step 2:** identify the information assets, the media in which they are represented and the systems that handle them.
- **Step 3:** identify the relationships between information assets, media, systems and organizational objectives.
- **Step 4:** identify those information assets, media and systems critical to organizational objectives.

These steps are identified on pages 73–74 of *IT Governance: A Manager's Guide to Data Security & BS 7799/ISO 177799* (the Set Book).

The definition of the scope of the ISMS, produced in Stage 1 of the ISMS documentation task, is used in Steps 1 and 2, to help identify the boundaries and the information assets.

Step 2 includes the identification of the owners, locations and security requirements of the information assets. The identification of the media and systems allows assets to be grouped according to the storage medium on which they are represented or according to the system(s) that handle them. This grouping of assets aids the execution of Steps 3 and 4 by allowing us to consider together all those assets represented on the same storage medium or handled by the same system(s). This grouping process is helpful not only during asset identification but also during risk assessment and treatment.

It is at Step 3 that the value of an information asset (or group of assets) to an organisation is determined: the greater the asset's contribution to organizational objectives, the greater its value to the organisation. In some circumstances it may be possible to assign a monetary or numerical value to an asset, but in the context of information security it is usually sufficient to classify the value as being low, medium or high (as in the classification of impact, likelihood and risk in the previous subsection). The value assigned to an asset can be useful in determining the impact of a breach of the security requirements of the asset.

The value assigned to an asset (or group of assets) feeds into Step 4 as a factor in determining those assets critical to organizational objectives. The importance of this step is that, in practice, it is unlikely that an organisation will have the resources to protect fully all of its assets. In these circumstances, risk assessment and treatment will need to focus on the critical assets, at least to begin with; other, non-critical assets can be protected later, if resources allow. At this step, it can often be useful to rank assets in an order of priority for risk assessment and treatment determined by how critical they are to organizational objectives.

## ***2.12 THE PDCA CYCLE***

In the previous section you were introduced to the nine-stage ISMS planning process advocated by the Standard. You have also, in Sections 7 and 8, looked in some detail at some of these stages – those comprising the ISMS documentation and asset identification tasks.

However, an ISMS must not only be planned, it must also be implemented, operated, monitored, reviewed, maintained and improved. Part 2 of the Standard provides guidance on these processes, which it suggests should be undertaken following a *Plan–Do–Check–Act* (PDCA) cycle. Here we introduce you to the PDCA cycle.

Walter Shewhart, a statistician working at Bell Laboratories in the 1930s, is credited with inventing the PDCA cycle. The PDCA cycle is the Standard's proposed methodology for the commission and continuous improvement of an ISMS. The PDCA cycle is also known as the **Denning cycle**, after the quality management guru **W Edwards Denning**.

Central to the PDCA cycle is the simple idea that we learn by doing. In the context of tackling a particular problem, the PDCA cycle relates to the idea that the act of building a solution to a problem leads to a better understanding of that problem, which can in turn lead to building a new and better solution, and so on. In its generic form, the PDCA cycle consists of the four iterated stages – Plan, Do, Check and Act – shown in Figure 50.

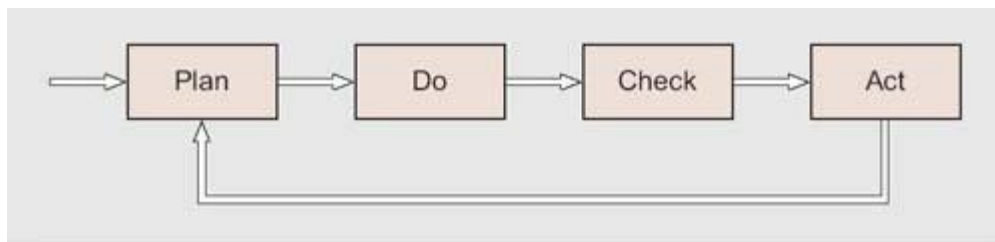


Figure 50 : The PDCA cycle<sup>73</sup>

The purpose of the **Plan** stage is to understand the problem and develop an initial, but fit-for-purpose, solution that can be created relatively quickly. Criteria against which the effectiveness of the initial and future solutions can be gauged are also agreed.

In the **Do** stage, the results of the Plan stage are implemented and then used. In the first iteration, this generally just means a pilot study to test the initial solution, so limiting any damage from mistakes in the Plan stage.

In the **Check** stage, the solution is observed in operation. The idea is to answer the following sorts of questions.

- Does the solution work in the way it was expected to? How well does it stand up against the evaluation criteria set up in the Plan stage?
- Has producing a solution changed our perception of the problem? Which parts of the problem do we understand well, and which parts not so well?

---

<sup>73</sup> <http://www.open.edu/openlearn/science-maths-technology/computing-and-ict/introduction-information-security/content-section-7>

- How could we change the solution to make it better? What changes would reflect our new perception of the problem? Which parts of the solution work well and which work poorly?

The answers to questions like these prepare for the **Act** stage, in which the current solution and the results of the Check stage are used to define a revised problem for initiating the Plan stage of the next iteration. Although not appropriate for all types of problem, the PDCA cycle does provide a way of tackling those problems:

- that exist in a complex and changing environment;
- that need an initial solution relatively quickly;
- for which there exist resources for continual improvement.

These characteristics certainly ought to apply to information security management. The PDCA cycle is a significant tool in an organization's work on information security management. However, it is beyond the scope of this course to discuss how it can be applied to ISMS management

## **2.13 SUMMARY**

This course has discussed the importance of information assets to any modern organisation and has made the case for information security management. It has introduced you to extracts from the British Standard on Information Security Management and to the approach advocated in the Standard for establishing and managing an information security management system (ISMS). It has also introduced the PDCA cycle. A particular focus in this course has been on the planning of ISMS, and on the four tasks and nine stages in this process. The course has considered in some detail the ISMS documentation and asset identification tasks.

## **2.14 CHECK YOUR PROGRESS**

- 1 \_\_\_\_\_ is the collection of technologies, standards, policies and management practices that are applied to information to keep it secure.
- 2 \_\_\_\_\_ comprises the meanings and interpretations that people place upon facts, or data.
- 3 \_\_\_\_\_ is the process by which the value of each of an organization's information assets is assessed and, if appropriate, protected on an ongoing basis.
- 4 The design of a successful information security policy and strategy for any organisation requires an assessment of a number of \_\_\_\_\_ .
- 5 As an organisation, it must meet stakeholders' expectations of \_\_\_\_\_, \_\_\_\_\_ and \_\_\_\_\_ of information.
- 6 In \_\_\_\_\_ information, an organisation also needs to be aware of the various laws, regulatory frameworks and codes of practice.
- 7 To maximize an information asset's utility (and thus its value) to an organisation, it should be available within its \_\_\_\_\_ region whenever needed.
- 8 The value of any piece of information relates to its levels of shareability and \_\_\_\_\_ .



- 9 The aim of information security is to preserve the value of information by ensuring that these levels are correctly identified and\_\_\_\_\_ .
- 10 \_\_\_\_\_ are the rewards and opportunities that arise from acting.
- 11 \_\_\_\_\_ are pressures that force you to act.
- 12 ISMS stands for \_\_\_\_\_.

## ***2.15 ANSWERS TO CHECK YOUR PROGRESS***

- 1 Information security
- 2 Information
- 3 Information Security Management
- 4 Key factors
- 5 continuity, confidentiality, privacy
- 6 sharing
- 7 shareability
- 8 Scarcity
- 9 Preserved
- 10 Incentives
- 11 Imperatives
- 12 Information Security Management System

## ***2.16 MODEL QUESTIONS***

1. List the main kinds of information a typical organisation requires to meet its mission.
2. How is information security characterized in the Standard?
3. How is information security achieved, according to the Standard?
4. Write down what you think 'ethical conduct' means in practice.
5. Which information assets, do you think, contribute most to (i) Coca-Cola's and (ii) Microsoft's value?
6. What precautions do you, or could you, take to assure yourself that there is no spyware on your computer at the moment?
7. Find out about your organization's current position on spyware and protection against it.
8. How much control does an organisation have over the shareability and scarcity regions of its information assets?
9. What are the possible results of a breach of the security requirements of an information asset?
10. Explain how the goals of shareability and scarcity for an information asset can be achieved in terms of the security requirements of confidentiality, integrity and availability.
11. Describe the personnel who should be involved in the development of an information security policy. Whom should the policy cover?
12. Describe the possible scopes of an ISMS.

13. Consider the role of an ISMS in protecting a collection of information assets, and explain how the scope of the ISMS relates to the shareability regions of the assets in such a collection.
14. Define 'threat' and 'attack' in relation to an information asset.
15. Distinguish between the 'outcome' of a threat and the 'impact' of an attack.
16. Describe, with examples, the possible types of threat to an information asset.
17. Describe the possible outcomes of a threat to an information asset, in each case stating which of the asset's security requirements has been breached.
18. Define the *vulnerability* of an information asset.
19. Define a risk combination table that is suitable for an organisation with few resources to allocate to security. What would be an acceptable level of risk for such an organisation?
20. Explain why:
  - (i) information assets and organizational objectives need to be related;
  - (ii) information assets need to be prioritized.
21. Explain PDCA cycle. Describe one or more areas of your life in which you use or could use the PDCA cycle.

## **UNIT III: CYBER SECURITY TECHNIQUES FOR SECURE E-COMMERCE**

### ***3.1 LEARNING OBJECTIVES***

After going through this unit a student will be able to understand:

- fo noitanifed eht wonKe-commerce.
- eht wonKHistory of e-commerce
- Understand the concerns of e-commerce
- tmemelpmI privacy and confidentiality in e-commerce.
- lamitpo tceleSSecurity solutions for e-commerce.
- mrofrepSecure Electronic Transactions.
- dnatsrednUFirewall Working of Antivirus software
- tuoba wonK Computer forensics
- dnatsrednU Steganography.

### ***3.2 ELECTRONIC COMMERCE***

Commonly written as **e-commerce**, is the trading in products or services using computer networks, such as the Internet. Electronic commerce draws on technologies such as mobile commerce, electronic funds transfer, supply chain management, Internet marketing, online transaction processing, electronic data interchange (EDI), inventory management systems, and automated data collection systems. Modern electronic commerce typically uses the World Wide Web for at least one part of the transaction's life cycle, although it may also use other technologies such as e-mail. E-commerce businesses may employ some or all of the following:

- Online shopping web sites for retail sales direct to consumers
- Providing or participating in online marketplaces, which process third-party business-to-consumer or consumer-to-consumer sales
- Business-to-business buying and selling
- Gathering and using demographic data through web contacts and social media
- Business-to-business electronic data interchange
- Marketing to prospective and established customers by e-mail or fax (for example, with newsletters)
- Engaging in pretail for launching new products and services

### ***3.3 HISTORY***

In 1998, IBM, with its agency Ogilvy & Mather, began to use its foundation in IT solutions and expertise to market itself as a leader of conducting business on the Internet through the term "**e-business**." Then CEO Louis V. Gerstner, Jr. was prepared to invest \$1 billion to market this new brand. After conducting worldwide market research in October 1997, IBM began with an eight-page piece in the Wall Street Journal that would introduce the concept of "e-business" and

advertise IBM's expertise in the new field. IBM decided not to trademark the term "e-business" in the hopes that other companies would use the term and create an entire new industry. However, this proved to be too successful and by 2000, to differentiate itself, IBM launched a \$300 million campaign about its "e-business infrastructure" capabilities. Since that time, the terms, "e-business" and "e-commerce" have been loosely interchangeable and have become a part of the common vernacular.

### ***3.4 BUSINESS MODEL***

When organizations go online, they have to decide which e-business models best suit their goals. A business model is defined as the organization of product, service and information flows, and the source of revenues and benefits for suppliers and customers. The concept of e-business model is the same but used in the online presence.

### ***3.5 REVENUE MODEL***

A key component of the business model is the revenue model, which is a framework for generating revenues. It identifies which revenue source to pursue, what value to offer, how to price the value, and who pays for the value. It is a key component of a company's business model. It primarily identifies what product or service will be created in order to generate revenues and the ways in which the product or service will be sold.

Without a well defined revenue model, that is, a clear plan of how to generate revenues, new businesses will more likely struggle due to costs which they will not be able to sustain. By having a clear revenue model, a business can focus on a target audience, fund development plans for a product or service, establish marketing plans, begin a line of credit and raise capital.

### ***3.6 CONCERNS***

While much has been written of the economic advantages of Internet-enabled commerce, there is also evidence that some aspects of the internet such as maps and location-aware services may serve to reinforce economic inequality and the digital divide. Electronic commerce may be responsible for consolidation and the decline of mom-and-pop, brick and mortar businesses resulting in increases in income inequality. Author Andrew Keen, a long-time critic of the social transformations caused by the Internet, has recently focused on the economic effects of consolidation from Internet businesses. Keen cites a 2013 Institute for Local Self-Reliance report saying brick-and-mortar retailers employ 47 people for every \$10 million in sales, while Amazon employs only 14. Similarly, the 700-employee room rental start-up Airbnb was valued at \$10 billion in 2014, about half as much as Hilton Hotels, which employs 152,000 people. And car-sharing Internet startup Uber employs 1,000 full-time employees and is valued at \$18.2 billion, about the same valuation as Avis and Hertz combined, which together employ almost 60,000 people.

### **3.6.1 Security**

E-Business systems naturally have greater security risks than traditional business systems, therefore it is important for e-business systems to be fully protected against these risks. A far greater number of people have access to e-businesses through the internet than would have access to a traditional business. Customers, suppliers, employees, and numerous other people use any particular e-business system daily and expect their confidential information to stay secure. Hackers are one of the great threats to the security of e-businesses. Some common security concerns for e-Businesses include keeping business and customer information private and confidential, authenticity of data, and data integrity. Some of the methods of protecting e-business security and keeping information secure include physical security measures as well as data storage, data transmission, anti-virus software, firewalls, and encryption to list a few.

### **3.6.2 Privacy and confidentiality**

Confidentiality is the extent to which businesses makes personal information available to other businesses and individuals. With any business, confidential information must remain secure and only be accessible to the intended recipient. However, this becomes even more difficult when dealing with e-businesses specifically. To keep such information secure means protecting any electronic records and files from unauthorized access, as well as ensuring safe transmission and data storage of such information. Tools such as encryption and firewalls manage this specific concern within e-business.

### **3.6.3 Authenticity**

E-business transactions pose greater challenges for establishing authenticity due to the ease with which electronic information may be altered and copied. Both parties in an e-business transaction want to have the assurance that the other party is who they claim to be, especially when a customer places an order and then submits a payment electronically. One common way to ensure this is to limit access to a network or trusted parties by using a virtual private network (VPN) technology. The establishment of authenticity is even greater when a combination of techniques are used, and such techniques involve checking "something you know" (i.e. password or PIN), "something you need" (i.e. credit card), or "something you are" (i.e. digital signatures or voice recognition methods). Many times in e-business, however, "something you are" is pretty strongly verified by checking the purchaser's "something you have" (i.e. credit card) and "something you know" (i.e. card number).

### **3.6.4 Data integrity**

Data integrity answers the question "Can the information be changed or corrupted in any way?" This leads to the assurance that the message received is identical to the message sent. A business needs to be confident that data is not changed in transit, whether deliberately or by accident. To help with data integrity, firewalls protect stored data against unauthorized access; while simply backing up data allows recovery should the data or equipment be damaged.

### **3.6.5 Non-repudiation**

This concern deals with the existence of proof in a transaction. A business must have assurance that the receiving party or purchaser cannot deny that a transaction has occurred, and this means having sufficient evidence to prove the transaction. One way to address non-repudiation is using digital signatures. A digital signature not only ensures that a message or document has been electronically signed by the person, but since a digital signature can only be created by one person, it also ensures that this person cannot later deny that they provided their signature.

### **3.6.6 Access control**

When certain electronic resources and information is limited to only a few authorized individuals, a business and its customers must have the assurance that no one else can access the systems or information. Fortunately, there are a variety of techniques to address this concern including firewalls, access privileges, user identification and authentication techniques (such as passwords and digital certificates), Virtual Private Networks (VPN), and much more.

### **3.6.7 Availability**

This concern is specifically pertinent to a business' customers as certain information must be available when customers need it. Messages must be delivered in a reliable and timely fashion, and information must be stored and retrieved as required. Because availability of service is important for all e-business websites, steps must be taken to prevent disruption of service by events such as power outages and damage to physical infrastructure. Examples to address this include data backup, fire-suppression systems, Uninterrupted Power Supply (UPS) systems, virus protection, as well as making sure that there is sufficient capacity to handle the demands posed by heavy network traffic.

## ***3.7 SECURITY SOLUTIONS***

When it comes to security solutions, sustainable electronic business requires support for data integrity, strong authentication, and privacy.

### **3.7.1 Access and data integrity**

There are several different ways to prevent access to the data that is kept online. One way is to use anti-virus software. This is something that most people use to protect their networks regardless of the data they have. E-businesses should use this because they can then be sure that the information sent and received to their system is clean. A second way to protect the data is to use firewalls and network protection. A firewall is used to restrict access to private networks, as well as public networks that a company may use. The firewall also has the ability to log attempts into the network and provide warnings as it is happening. They are very beneficial to keep third-parties out of the network. Businesses that use Wi-Fi need to consider different forms of protection because these networks are easier for someone to access. They should look into protected access, virtual private networks, or internet protocol security. Another option they have is an intrusion detection system. This system alerts when there are possible intrusions. Some

companies set up traps or "hot spots" to attract people and are then able to know when someone is trying to hack into that area.

### **3.7.2 Encryption**

Encryption, which is actually a part of cryptography, involves transforming texts or messages into a code which is unreadable. These messages have to be decrypted in order to be understandable or usable for someone. There is a key that identifies the data to a certain person or company. With public key encryption, there are actually two keys used. One is public and one is private. The public one is used for encryption, and the private for decryption. The level of the actual encryption can be adjusted and should be based on the information. The key can be just a simple slide of letters or a completely random mix-up of letters. This is relatively easy to implement because there is software that a company can purchase. A company needs to be sure that their keys are registered with a certificate authority.

### **3.7.3 Digital certificates**

The point of a digital certificate is to identify the owner of a document. This way the receiver knows that it is an authentic document. Companies can use these certificates in several different ways. They can be used as a replacement for user names and passwords. Each employee can be given these to access the documents that they need from wherever they are. These certificates also use encryption. They are a little more complicated than normal encryption however. They actually used important information within the code. They do this in order to assure authenticity of the documents as well as confidentiality and data integrity which always accompany encryption. Digital certificates are not commonly used because they are confusing for people to implement. There can be complications when using different browsers, which mean they need to use multiple certificates. The process is being adjusted so that it is easier to use.

### **3.7.4 Digital signatures**

A final way to secure information online would be to use a digital signature. If a document has a digital signature on it, no one else is able to edit the information without being detected. That way if it is edited, it may be adjusted for reliability after the fact. In order to use a digital signature, one must use a combination of cryptography and a message digest. A message digest is used to give the document a unique value. That value is then encrypted with the sender's private key.

## ***3.8 E-COMMERCE IDENTIFICATION AND IDENTIFICATION TYPES***

A whole new range of techniques has been developed to identify people since the 1960s from the measurement and analysis of parts of their bodies to DNA profiles. Forms of identification are used to ensure that citizens are eligible for rights to benefits and to vote without fear of impersonation while private individuals have used seals and signatures for centuries to lay claim to real and personal estate.“ Generally, the amount of proof of identity that is required to gain access to something is proportionate to the value of what is being sought." It is estimated that

only 4% of online transactions use methods other than simple passwords. Security of systems resources generally follow a three-step process of “**identification, authentication and authorization**”. Today, a high level of trust is as critical to e-Commerce transactions as it is to traditional face-to-face transactions.

### ***3.9 IDENTIFICATION, AUTHENTICATION AND AUTHORIZATION***

#### **3.9.1 Identification**

It is a scheme established and maintained, whereby users are properly, consistently, effectively and efficiently identified before systems are accessed.

#### **3.9.2 Authentication**

Authentication is verification of the identity of the entity requesting access to a system. It is the process of determining whether someone or something is, in fact, who or what it is declared to be. In private and public computer networks (including the Internet), authentication is commonly done through the use of logon passwords. Knowledge of the password is assumed to guarantee that the user is authentic. Each user registers initially (or is registered by someone else), using an assigned or self-declared password. On each subsequent use, the user must know and use the previously declared password. The weakness in this system for transactions that are significant (such as the exchange of money) is that passwords can often be stolen, accidentally revealed, or forgotten. For this reason, Internet business and many other transactions require a more stringent authentication process. The use of digital certificates issued and verified by a Certificate Authority (CA) as part of a public key infrastructure is considered likely to become the standard way to perform authentication on the Internet. Logically, authentication precedes authorization (although they may often seem to be combined).

#### **3.9.3 Authorization**

Authorization is the process of giving someone permission to do or have something. In multi-user computer systems, a system administrator defines for the system which users are allowed access to the system and what privileges of use (such as access to which file directories, hours of access, amount of allocated storage space, and so forth). Assuming that someone has logged in to a computer operating system or application, the system or application may want to identify what resources the user can be given during this session. Thus, authorization is sometimes seen as both the preliminary setting up of permissions by a system administrator and the actual checking of the permission values that have been set up when a user is getting access. Logically, authorization is preceded by authentication. ).

### ***3.10 TYPES OF ECOMMERCE AUTHENTICATION***

- **One-time password/Single sign on** - It is process where a user's password and information is used for logon and then, becomes invalid after a set time.



- **Two-factor authentication** - This requires two forms of authentication before access can be granted to a user.
- **Multi-factor authentication** - Multi-factor authentication requires that the user uses a user id, password combined with any other form of authentication method as smartcard or biometric. Using this method decreases the likelihood that an unauthorized person can compromise your electronic security system, but it also increases the cost of maintaining that system.
- **Electronic access card/Smart card** - Smart cards are credit card-sized plastic cards that house an embedded integrated circuit. They can be used in electronic commerce for providing personal security, stored value and mobility. At the functional level, smart cards can be categorized as either memory cards or microprocessor cards. Memory cards, such as disposable pre-paid payphone cards or loyalty card, are the most cheapest form of smart card. They contain a small amount of memory in the form of ROM (read only memory) and EEPROM (electrically erasable programmable read only memory). Microprocessor cards are more advanced than simple memory cards in that they contain a microprocessor CPU (central processing unit) and RAM (random access memory) in addition to ROM and EEPROM. The ROM contains the card's operating system and factory-loaded applications.
- **Security token** - It is an authentication device that has been assigned to a specific user by an appropriate administrator". It uses what the user has such as, Passport, driver's license etc. to identify them. "Most security tokens also incorporate two-factor authentication methods to work effectively".
- **Keystroke dynamics** - It is an automated form of authentication based on something the user does. It authenticates the user based keyboard typing pattern.
- **Biometric** - Biometric based systems enable the automatic identification and/or authentication of individuals. Authentication answers the question: "Am I who I claim to be"? The system verifies the identity of the person by processing biometric data, which refers to the person who asks and takes a yes/no decision (1:1 comparison). On the other hand, identification answers to the question: "Who am I?". The system recognizes the individual who asks by distinguishing him from other persons whose biometric data is also stored in the database. In this case the system takes a 1-of-n decision, and answers that the person who asks is X, if her/his biometric data is stored in the database or that there is no match at all. Although the identification function should be regarded as distinct from authentication from an application perspective, often systems using biometrics integrate both identification and authentication functions, since the former is a repetitive execution of the latter.

### ***3.11 TYPES OOF BIOMETRIC AUTHENTICATION***

- **Fingerprint recognition** - Fingerprint is the most widely used form of authentication where the pattern of a user's fingertip is used. It can be deployed in a broad range of

environments and provides flexibility and increased system accuracy by allowing users to enrol multiple fingers in the template system.

- **Facial recognition** - It uses data related to the unique facial features of a user. It involves analyzing facial characteristics. It is a unique biometric in that it does not require the cooperation of the scanned individual; it can utilize almost any high-resolution image acquisition device such as a still or motion camera.
- **Voice pattern** - This a form of authentication uses the unique pattern of a user's voice. it relies on voice-to-print technologies, not voice recognition. In this process, a persons voice is transformed into text and compared to an original template. Although this is fairly easy technology to implement because many computers already have built-in microphones, the enrollment procedure is more complicated than other biometrics, and background noise can interfere with the scanning, which can be frustrating to the user.
- **Handwritten Signature** - Signature verification analysis the way a person signs their name, such as speed and pressure, as well as the final static shape of the signature itself.
- **Retina recognition** - It is a method of biometric authentication that uses data related to unique characteristics associated with the pattern of blood vessels located at the back of an individual's eyes. This technology is personally invasive and requires skilled operators. It results in retina codes of 96 bytes when used for authentication to some Kbytes in the case of identification. Facial recognition techniques exploit characteristics such as relative eyes, nose and mouth positioning, and the distances between them.
- **Iris recognition** - A form of authentication that uses data linked to features associated with the colored part of the eye of a user. It involves analyzing the patterns of the colored part of the eye surrounding the pupil. It uses a fairly normal camera and does not require close contact between the eye and the scanner. Glasses can be worn during an iris scan, unlike a retinal scan.

### ***3.12 OTHER FORMS OF AUTHENTICATION***

- **Mutual Authentication** - is the process by which each party in an electronic communication verifies the identity of the other. For instance, a bank clearly has an interest in positively identifying an account holder prior to allowing a transfer of funds; however, the bank customer also have a financial interest in knowing he is communicating with the bank's server prior to providing any personal information.
- **Digital certificate** - A digital certificate is an electronic "credit card" that establishes your credentials when doing business or other transactions on the Web. It is issued by a certification authority (CA). It contains your name, a serial number, expiration dates, a copy of the certificate holder's public key (used for encrypting messages and digital signatures), and the digital signature of the certificate-issuing authority so that a recipient can verify that the certificate is real. Some digital certificates conform to a standard, X.509. Digital certificates can be kept in registries so that authenticating users can look up other users' public keys. ).[8] Digital certificates are used in a variety of transactions including e-mail, electronic commerce, and the electronic transfer of funds. When

combined with encryption and digital signatures, digital certificates provide individuals and organizations with a means of privately sharing information so that each party is confident that the individual or organization with which they are communicating is in fact who it claims to be.

- **Hand Geometry Authentication** - Hand geometry techniques exploit hand shape characteristics, such as finger length and width. This leads to quite a small amount of data (about 9 bytes), thus restricting their application to simple authentication purposes only. Also, their behaviour related to the fulfilment of the above properties is moderate. The iris, the circular coloured membrane surrounding the pupil of the eye, is a unique structure consisting of specific characteristics such as striations, furrows, rings, crypts, filaments, and corona. Iris patterns are characterised by very high distinctiveness, even twins have different ones. The probability that two individuals have the same iris pattern is about  $10^{\sup -52}$ . The probability that two distinct iris patterns result to the same iris-code used (about 256 bytes) by a biometric system is negligible (about  $10^{\sup -78}$ ), thus allowing almost perfect matching accuracy.
- **Kerberos authentication** - This is a form of authentication that provides a mechanism for authenticating a client and a server or server to a server.
- **CHAP authentication** - This is form of peer-to-peer protocol (PPP) mechanism used by an authenticator to authenticate a peer.
- **Quantitative authentication** - Quantitative authentication is an authentication approach where someone requesting access is required to attain a certain "authentication level" before being granted access. Detailed discussions on quantitative authentication have been undertaken.

### ***3.13 SECURE ELECTRONIC TRANSACTION***

Secure Electronic Transaction (SET) was a communications protocol standard for securing credit card transactions over insecure networks, specifically, the Internet. SET was not itself a payment system, but rather a set of security protocols and formats that enabled users to employ the existing credit card payment infrastructure on an open network in a secure fashion. However, it failed to gain attraction in the market. VISA now promotes the 3-D Secure scheme.

#### **3.13.1 History and development**

SET was developed by the SET Consortium, established in 1996 by VISA and MasterCard in cooperation with GTE, IBM, Microsoft, Netscape, SAIC, Terisa Systems, RSA, and VeriSign. The consortium's goal was to combine the card associations' similar but incompatible protocols (STT from Visa/Microsoft and SEPP from MasterCard/IBM) into a single standard. SET allowed parties to identify themselves to each other and exchange information securely. Binding of identities was based on X.509 certificates with several extensions. SET used a cryptographic blinding algorithm that, in effect, would have let merchants substitute a certificate for a user's credit-card number. If SET were used, the merchant itself would never have had to know the credit-card numbers being sent from the buyer, which would have provided verified good

payment but protected customers and credit companies from fraud. SET was intended to become the de facto standard payment method on the Internet between the merchants, the buyers, and the credit-card companies.

### 3.13.2 Key features

To meet the business requirements, SET incorporates the following features:

- Confidentiality of information
- Integrity of data
- Cardholder account authentication
- Merchant authentication

### 3.13.3 Participants

A SET system includes the following participants:

- Cardholder
- Merchant
- Issuer
- Acquirer
- Payment gateway
- Certification authority

### 3.13.4 How it Works

Both cardholders and merchants must register with CA (certificate authority) first, before they can buy or sell on the Internet, which we will talk about later. Once registration is done, cardholder and merchant can start to do transactions, which involve 9 basic steps in this protocol, which is simplified.

1. Customer browses website and decides on what to purchase
2. Customer sends order and payment information, which includes 2 parts in one message:
  - a. Purchase Order – this part is for merchant
  - b. Card Information – this part is for merchant's bank only.
3. Merchant forwards card information (part b) to their bank
4. Merchant's bank checks with Issuer for payment authorization
5. Issuer sends authorization to Merchant's bank
6. Merchant's bank send authorization to merchant
7. Merchant completes the order and sends confirmation to the customer
8. Merchant captures the transaction from their bank
9. Issuer prints credit card bill (invoice) to customer

### 3.13.5 Dual signature

As described in (Stallings 2000):

“An important innovation introduced in SET is the dual signature. The purpose of the dual signature is to link two messages that are intended for two different recipients. In this case, the customer wants to send the **order information** (OI) to the merchant and the **payment information** (PI) to the bank. The merchant does not need to know the customer's credit-card

number, and the bank does not need to know the details of the customer's order. The customer is afforded extra protection in terms of privacy by keeping these two items separate. However, the two items must be linked in a way that can be used to resolve disputes if necessary. The link is needed so that the customer can prove that this payment is intended for this order and not for some other goods or service.”

The message digest (MD) of the OI and the PI are independently calculated by the customer. The dual signature is the encrypted MD (with the customer's secret key) of the concatenated MD's of PI and OI. The dual signature is sent to both the merchant and the bank. The protocol arranges for the merchant to see the MD of the PI without seeing the PI itself, and the bank sees the MD of the OI but not the OI itself. The dual signature can be verified using the MD of the OI or PI. It doesn't require the OI or PI itself. Its MD does not reveal the content of the OI or PI, and thus privacy is preserved.

### **3.13.6 Digital signature**

A digital signature is a mathematical scheme for demonstrating the authenticity of a digital message or documents. A valid digital signature gives a recipient reason to believe that the message was created by a known sender, that the sender cannot deny having sent the message (authentication and non-repudiation), and that the message was not altered in transit (integrity). Digital signatures are commonly used for software distribution, financial transactions, and in other cases where it is important to detect forgery or tampering.

#### **3.13.6.1 Explanation**

Digital signatures are often used to implement electronic signatures, a broader term that refers to any electronic data that carries the intent of a signature, but not all electronic signatures use digital signatures. In some countries, including the United States, India, Brazil, Saudi Arabia and members of the European Union, electronic signatures have legal significance. Digital signatures employ asymmetric cryptography. In many instances they provide a layer of validation and security to messages sent through a non-secure channel: Properly implemented, a digital signature gives the receiver reason to believe the message was sent by the claimed sender. Digital seals and signatures are equivalent to handwritten signatures and stamped seals. Digital signatures are equivalent to traditional handwritten signatures in many respects, but properly implemented digital signatures are more difficult to forge than the handwritten type. Digital signature schemes, in the sense used here, are cryptographically based, and must be implemented properly to be effective. Digital signatures can also provide non-repudiation, meaning that the signer cannot successfully claim they did not sign a message, while also claiming their private key remains secret; further, some non-repudiation schemes offer a time stamp for the digital signature, so that even if the private key is exposed, the signature is valid. Digitally signed messages may be anything representable as a bitstring: examples include electronic mail, contracts, or a message sent via some other cryptographic protocol.

A digital signature scheme typically consists of three algorithms;

- A key generation algorithm that selects a private key uniformly at random from a set of possible private keys. The algorithm outputs the private key and a corresponding public key.
- A signing algorithm that, given a message and a private key, produces a signature.
- A signature verifying algorithm that, given the message, public key and signature, either accepts or rejects the message's claim to authenticity.

Two main properties are required. First, the authenticity of a signature generated from a fixed message and fixed private key can be verified by using the corresponding public key. Secondly, it should be computationally infeasible to generate a valid signature for a party without knowing that party's private key. A digital signature is an authentication mechanism that enables the creator of the message to attach a code that acts as a signature.

### 3.13.6.2 How they work

To create RSA signature keys, generate an RSA key pair containing a modulus  $N$  that is the product of two large primes, along with integers  $e$  and  $d$  such that  $ed \equiv 1 \pmod{\phi(N)}$ , where  $\phi$  is the Euler phi-function. The signer's public key consists of  $N$  and  $e$ , and the signer's secret key contains  $d$ .

To sign a message  $m$ , the signer computes  $\sigma \equiv md \pmod{N}$ . To verify, the receiver checks that  $\sigma e \equiv m \pmod{N}$ .

As noted earlier, this basic scheme is not very secure. To prevent attacks, one can first apply a cryptographic hash function to the message  $m$  and then apply the RSA algorithm described above to the result. This approach can be proven secure in the so-called random oracle model[clarification needed]. Most early signature schemes were of a similar type: they involve the use of a trapdoor permutation, such as the RSA function, or in the case of the Rabin signature scheme, computing square modulo composite  $n$ . A trapdoor permutation family is a family of permutations, specified by a parameter, that is easy to compute in the forward direction, but is difficult to compute in the reverse direction without already knowing the private key ("trapdoor"). Trapdoor permutations can be used for digital signature schemes, where computing the reverse direction with the secret key is required for signing, and computing the forward direction is used to verify signatures.

Used directly, this type of signature scheme is vulnerable to a key-only existential forgery attack. To create a forgery, the attacker picks a random signature  $\sigma$  and uses the verification procedure to determine the message  $m$  corresponding to that signature. In practice, however, this type of signature is not used directly, but rather, the message to be signed is first hashed to produce a short digest that is then signed. This forgery attack, then, only produces the hash function output that corresponds to  $\sigma$ , but not a message that leads to that value, which does not lead to an attack. In the random oracle model, this hash-then-sign form of signature is existentially unforgeable, even against a chosen-plaintext attack. There are several reasons to sign such a hash (or message digest) instead of the whole document.

- For efficiency: The signature will be much shorter and thus save time since hashing is generally much faster than signing in practice.
- For compatibility: Messages are typically bit strings, but some signature schemes operate on other domains (such as, in the case of RSA, numbers modulo a composite number  $N$ ). A hash function can be used to convert an arbitrary input into the proper format.
- For integrity: Without the hash function, the text "to be signed" may have to be split (separated) in blocks small enough for the signature scheme to act on them directly. However, the receiver of the signed blocks is not able to recognize if all the blocks are present and in the appropriate order.

### 3.13.7 Notions of security

In their foundational paper, Goldwasser, Micali, and Rivest lay out a hierarchy of attack models against digital signatures:

1. In a key-only attack, the attacker is only given the public verification key.
2. In a known message attack, the attacker is given valid signatures for a variety of messages known by the attacker but not chosen by the attacker.
3. In an adaptive chosen message attack, the attacker first learns signatures on arbitrary messages of the attacker's choice.

They also describe a hierarchy of attack results:

1. A total break results in the recovery of the signing key.
2. A universal forgery attack results in the ability to forge signatures for any message.
3. A selective forgery attack results in a signature on a message of the adversary's choice.
4. An existential forgery merely results in some valid message/signature pair not already known to the adversary.

The strongest notion of security, therefore, is security against existential forgery under an adaptive chosen message attack.

### 3.13.8 Applications of digital signatures

As organizations move away from paper documents with ink signatures or authenticity stamps, digital signatures can provide added assurances of the evidence to provenance, identity, and status of an electronic document as well as acknowledging informed consent and approval by a signatory. The United States Government Printing Office (GPO) publishes electronic versions of the budget, public and private laws, and congressional bills with digital signatures. Universities including Penn State, University of Chicago, and Stanford are publishing electronic student transcripts with digital signatures. Below are some common reasons for applying a digital signature to communications:

#### 3.13.8.1 Authentication

Although messages may often include information about the entity sending a message, that information may not be accurate. Digital signatures can be used to authenticate the source of messages. When ownership of a digital signature secret key is bound to a specific user, a valid signature shows that the message was sent by that user. The importance of high confidence in

sender authenticity is especially obvious in a financial context. For example, suppose a bank's branch office sends instructions to the central office requesting a change in the balance of an account. If the central office is not convinced that such a message is truly sent from an authorized source, acting on such a request could be a grave mistake.

### **3.13.8.2 Integrity**

In many scenarios, the sender and receiver of a message may have a need for confidence that the message has not been altered during transmission. Although encryption hides the contents of a message, it may be possible to change an encrypted message without understanding it. (Some encryption algorithms, known as nonmalleable ones, prevent this, but others do not.) However, if a message is digitally signed, any change in the message after signature invalidates the signature. Furthermore, there is no efficient way to modify a message and its signature to produce a new message with a valid signature, because this is still considered to be computationally infeasible by most cryptographic hash functions (see collision resistance).

### **3.13.8.3 Non-repudiation**

Non-repudiation, or more specifically non-repudiation of origin, is an important aspect of digital signatures. By this property, an entity that has signed some information cannot at a later time deny having signed it. Similarly, access to the public key only does not enable a fraudulent party to fake a valid signature.

Note that these authentications, non-repudiation etc. properties rely on the secret key not having been revoked prior to its usage. Public revocation of a key-pair is a required ability; else leaked secret keys would continue to implicate the claimed owner of the key-pair. Checking revocation status requires an "online" check, e.g. checking a "Certificate Revocation List" or via the "Online Certificate Status Protocol". Very roughly this is analogous to a vendor who receives credit-cards first checking online with the credit-card issuer to find if a given card has been reported lost or stolen. Of course, with stolen key pairs, the theft is often discovered only after the secret key's use, e.g., to sign a bogus certificate for espionage purpose.

## ***3.14 ADDITIONAL SECURITY PRECAUTIONS***

### **3.14.1 Putting the private key on a smart card**

All public key / private key cryptosystems depend entirely on keeping the private key secret. A private key can be stored on a user's computer, and protected by a local password, but this has two disadvantages:

- the user can only sign documents on that particular computer
- the security of the private key depends entirely on the security of the computer

A more secure alternative is to store the private key on a smart card. Many smart cards are designed to be tamper-resistant (although some designs have been broken, notably by Ross Anderson and his students). In a typical digital signature implementation, the hash calculated from the document is sent to the smart card, whose CPU signs the hash using the stored private



key of the user, and then returns the signed hash. Typically, a user must activate his smart card by entering a personal identification number or PIN code (thus providing two-factor authentication). It can be arranged that the private key never leaves the smart card, although this is not always implemented. If the smart card is stolen, the thief will still need the PIN code to generate a digital signature. This reduces the security of the scheme to that of the PIN system, although it still requires an attacker to possess the card. A mitigating factor is that private keys, if generated and stored on smart cards, are usually regarded as difficult to copy, and are assumed to exist in exactly one copy. Thus, the loss of the smart card may be detected by the owner and the corresponding certificate can be immediately revoked. Private keys that are protected by software only may be easier to copy, and such compromises are far more difficult to detect.

### **3.14.2 Using smart card readers with a separate keyboard**

Entering a PIN code to activate the smart card commonly requires a numeric keypad. Some card readers have their own numeric keypad. This is safer than using a card reader integrated into a PC, and then entering the PIN using that computer's keyboard. Readers with a numeric keypad are meant to circumvent the eavesdropping threat where the computer might be running a keystroke logger, potentially compromising the PIN code. Specialized card readers are also less vulnerable to tampering with their software or hardware and are often EAL3 certified.

### **3.14.3 Other smart card designs**

Smart card design is an active field, and there are smart card schemes which are intended to avoid these particular problems, though so far with little security proofs.

### **3.14.4 Using digital signatures only with trusted applications**

One of the main differences between a digital signature and a written signature is that the user does not "see" what he signs. The user application presents a hash code to be signed by the digital signing algorithm using the private key. An attacker who gains control of the user's PC can possibly replace the user application with a foreign substitute, in effect replacing the user's own communications with those of the attacker. This could allow a malicious application to trick a user into signing any document by displaying the user's original on-screen, but presenting the attacker's own documents to the signing application. To protect against this scenario, an authentication system can be set up between the user's application (word processor, email client, etc.) and the signing application. The general idea is to provide some means for both the user application and signing application to verify each other's integrity. For example, the signing application may require all requests to come from digitally signed binaries.

### **3.14.5 Using a network attached hardware security module**

One of the main differences between a cloud based digital signature service and a locally provided one is risk. Many risk averse companies, including governments, financial and medical institutions, and payment processors require more secure standards, like FIPS 140-2 level 3 and FIPS 201 certification, to ensure the signature is validated and secure.

Technically speaking, a digital signature applies to a string of bits, whereas humans and applications "believe" that they sign the semantic interpretation of those bits. In order to be semantically interpreted, the bit string must be transformed into a form that is meaningful for humans and applications, and this is done through a combination of hardware and software based processes on a computer system. The problem is that the semantic interpretation of bits can change as a function of the processes used to transform the bits into semantic content. It is relatively easy to change the interpretation of a digital document by implementing changes on the computer system where the document is being processed. From a semantic perspective this creates uncertainty about what exactly has been signed. WYSIWYS (What You See Is What You Sign) means that the semantic interpretation of a signed message cannot be changed. In particular this also means that a message cannot contain hidden information that the signer is unaware of, and that can be revealed after the signature has been applied. WYSIWYS is a necessary requirement for the validity of digital signatures, but this requirement is difficult to guarantee because of the increasing complexity of modern computer systems.

### ***3.15 DIGITAL SIGNATURES VERSUS INK ON PAPER SIGNATURES***

An ink signature could be replicated from one document to another by copying the image manually or digitally, but to have credible signature copies that can resist some scrutiny is a significant manual or technical skill, and to produce ink signature copies that resist professional scrutiny is very difficult. Digital signatures cryptographically bind an electronic identity to an electronic document and the digital signature cannot be copied to another document. Paper contracts sometimes have the ink signature block on the last page, and the previous pages may be replaced after a signature is applied. Digital signatures can be applied to an entire document, such that the digital signature on the last page will indicate tampering if any data on any of the pages have been altered, but this can also be achieved by signing with ink and numbering all pages of the contract.

#### **3.15.1 Some digital signature algorithms**

- RSA-based signature schemes, such as RSA-PSS
- DSA and its elliptic curve variant ECDSA
- ElGamal signature scheme as the predecessor to DSA, and variants Schnorr signature and Pointcheval–Stern signature algorithm
- Rabin signature algorithm
- Pairing-based schemes such as BLS
- Undeniable signatures
- Aggregate signature - a signature scheme that supports aggregation: Given  $n$  signatures on  $n$  messages from  $n$  users, it is possible to aggregate all these signatures into a single signature whose size is constant in the number of users. This single signature will convince the verifier that the  $n$  users did indeed sign the  $n$  original messages.

- Signatures with efficient protocols - are signature schemes that facilitate efficient cryptographic protocols such as zero-knowledge proofs or secure computation.

### ***3.16 THE CURRENT STATE OF USE- LEGAL AND PRACTICAL***

All digital signature schemes share the following basic prerequisites regardless of cryptographic theory or legal provision:

1. Quality algorithms: Some public-key algorithms are known to be insecure, practical attacks against them having been discovered.
2. Quality implementations: An implementation of a good algorithm (or protocol) with mistake(s) will not work.
3. The private key must remain private: If the private key becomes known to any other party, that party can produce perfect digital signatures of anything whatsoever.
4. The public key owner must be verifiable: A public key associated with Bob actually came from Bob. This is commonly done using a public key infrastructure (PKI) and the public key↔user association is attested by the operator of the PKI (called a certificate authority). For 'open' PKIs in which anyone can request such an attestation (universally embodied in a cryptographically protected identity certificate), the possibility of mistaken attestation is nontrivial. Commercial PKI operators have suffered several publicly known problems. Such mistakes could lead to falsely signed, and thus wrongly attributed, documents. 'Closed' PKI systems are more expensive, but less easily subverted in this way.
5. Users (and their software) must carry out the signature protocol properly.

Only if all of these conditions are met will a digital signature actually be any evidence of who sent the message, and therefore of their assent to its contents. Legal enactment cannot change this reality of the existing engineering possibilities, though some such have not reflected this actuality. Legislatures, being importuned by businesses expecting to profit from operating a PKI, or by the technological avant-garde advocating new solutions to old problems, have enacted statutes and/or regulations in many jurisdictions authorizing, endorsing, encouraging, or permitting digital signatures and providing for (or limiting) their legal effect. The first appears to have been in Utah in the United States, followed closely by the states Massachusetts and California. Other countries have also passed statutes or issued regulations in this area as well and the UN has had an active model law project for some time. These enactments (or proposed enactments) vary from place to place, have typically embodied expectations at variance (optimistically or pessimistically) with the state of the underlying cryptographic engineering, and have had the net effect of confusing potential users and specifiers, nearly all of whom are not cryptographically knowledgeable. Adoption of technical standards for digital signatures have lagged behind much of the legislation, delaying a more or less unified engineering position on interoperability, algorithm choice, key lengths, and so on what the engineering is attempting to provide.

### 3.17 INDUSTRY STANDARDS

Some industries have established common interoperability standards for the use of digital signatures between members of the industry and with regulators. These include the Automotive Network Exchange for the automobile industry and the SAFE-BioPharma Association for the healthcare industry.

#### 3.17.1 Using separate key pairs for signing and encryption

In several countries, a digital signature has a status somewhat like that of a traditional pen and paper signature, like in the EU digital signature legislation. Generally, these provisions mean that anything digitally signed legally binds the signer of the document to the terms therein. For that reason, it is often thought best to use separate key pairs for encrypting and signing. Using the encryption key pair, a person can engage in an encrypted conversation (e.g., regarding a real estate transaction), but the encryption does not legally sign every message he sends. Only when both parties come to an agreement do they sign a contract with their signing keys, and only then are they legally bound by the terms of a specific document. After signing, the document can be sent over the encrypted link. If a signing key is lost or compromised, it can be revoked to mitigate any future transactions. If an encryption key is lost, a backup or key escrow should be utilized to continue viewing encrypted content. Signing keys should never be backed up or escrowed unless the backup destination is securely encrypted.

### 3.18 ANTIVIRUS SOFTWARE

ClamTk, an open source antivirus based on the ClamAV antivirus engine, originally developed by Tomasz Kojm in 2001. Antivirus or anti-virus software (often abbreviated as AV), sometimes known as anti-malware software, is computer software used to prevent, detect and remove malicious software. Antivirus software was originally developed to detect and remove computer viruses, hence the name.



Figure 51: Open source antivirus, ClamTk<sup>74</sup>

<sup>74</sup> .ysetruoc egam|https://en.wikipedia.org/wiki/File:ClamTK.3.08.jpg

However, with the proliferation of other kinds of malware, antivirus software started to provide protection from other computer threats. In particular, modern antivirus software can protect from: malicious Browser Helper Objects (BHOs), browser hijackers, ransomware, keyloggers, backdoors, rootkits, trojan horses, worms, malicious LSPs, dialers, fraudtools, adware and spyware. Some products also include protection from other computer threats, such as infected and malicious URLs, spam, scam and phishing attacks, online identity (privacy), online banking attacks, social engineering techniques, Advanced Persistent Threat (APT), botnets DDoS attacks.

### **3.18.1 Identification methods for viruses**

One of the few solid theoretical results in the study of computer viruses is Frederick B. Cohen's 1987 demonstration that there is no algorithm that can perfectly detect all possible viruses. However, using different layer of defense, a good detection rate may be achieved. There are several methods which antivirus engine can use to identify malware:

- Signature-based detection: is the most common method. To identify viruses and other malware, the antivirus engine compares the contents of a file to its database of known malware signatures.
- Heuristic-based detection: is generally used together with signature-based detection. It detects malware based on characteristics typically used in known malware code.
- Behavioural-based detection: is similar to heuristic-based detection and used also in Intrusion Detection System. The main difference is that, instead of characteristics hardcoded in the malware code itself, it is based on the behavioural fingerprint of the malware at run-time. Clearly, this technique is able to detect (known or unknown) malware only after they have starting doing their malicious actions.
- Sandbox detection: is a particular behavioural-based detection technique that, instead of detecting the behavioural fingerprint at run time, it executes the programs in a virtual environment, logging what actions the program performs. Depending on the actions logged, the antivirus engine can determine if the program is malicious or not. If not, then, the program is executed in the real environment. Albeit this technique has shown to be quite effective, given its heaviness and slowness, it is rarely used in end-user antivirus solutions.
- Data mining techniques: are one of the latest approach applied in malware detection. Data mining and machine learning algorithms are used to try to classify the behaviour of a file (as either malicious or benign) given a series of file features, that are extracted from the file itself.

### **3.18.2 Signature-based detection**

Traditional antivirus software relies heavily upon signatures to identify malware. Substantially, when a malware arrives in the hands of an antivirus firm, it is analysed by malware researchers or by dynamic analysis systems. Then, once it is determined to be a malware, a proper signature of the file is extracted and added to the signatures database of the antivirus software. When a particular file has to be scanned, the antivirus engine compares the contents of the file with all the malware signatures in the signatures database. If the file matches one signature, then the

engine knows which malware it is and which procedure has to be performed in order to clean the infection.

Signature-based detection technique can be very effective but, clearly, cannot defend against malware unless some of its samples have already been obtained, a proper signature generated and the antivirus product updated. Signature-based detection systems rely on the premise that, generally speaking, the more infective a malware is the faster arrives in the hands of security researchers. Thus, even if it does not guarantee perfection, it protects from the most widespread threats. However, this approach is not really effective against zero-day or next-generation malware, i.e. malware that has not been yet encountered/analysed.

As new malware are being created each day, the signature-based detection approach requires frequent updates of the signatures database. To assist the antivirus firms, the software may automatically upload new malware to the company or allow the user to manually do it, allowing the antivirus firms to dramatically shorten the life of those threats. Some antivirus products includes also advanced software to spot zero-day or next-generation malware.[citation needed]

Although the signature-based approach can effectively contain malware outbreaks, malware authors have tried to stay a step ahead of such software by writing "oligomorphic", "polymorphic" and, more recently, "metamorphic" viruses, which encrypt parts of themselves or otherwise modify themselves as a method of disguise, so as to not match virus signatures in the dictionary.

### **3.18.3 Heuristics**

Some more sophisticated antivirus software uses heuristic analysis to identify new malware or variants of known malware. Many viruses start as a single infection and through either mutation or refinements by other attackers, can grow into dozens of slightly different strains, called variants. Generic detection refers to the detection and removal of multiple threats using a single virus definition. For example, the Vundotrojan has several family members, depending on the antivirus vendor's classification. Symantec classifies members of the Vundo family into two distinct categories, Trojan.Vundo and Trojan.Vundo.B. While it may be advantageous to identify a specific virus, it can be quicker to detect a virus family through a generic signature or through an inexact match to an existing signature. Virus researchers find common areas that all viruses in a family share uniquely and can thus create a single generic signature. These signatures often contain non-contiguous code, using wildcard characters where differences lie. These wildcards allow the scanner to detect viruses even if they are padded with extra, meaningless code. A detection that uses this method is said to be "heuristic detection."

### **3.18.4 Rootkit detection**

Anti-virus software can attempt to scan for rootkits. A rootkit is a type of malware designed to gain administrative-level control over a computer system without being detected. Rootkits can

change how the operating system functions and in some cases can tamper with the anti-virus program and render it ineffective. Rootkits are also difficult to remove, in some cases requiring a complete re-installation of the operating system.

### **3.18.5 Real-time protection**

Real-time protection, on-access scanning, background guard, resident shield, autoprotect, and other synonyms refer to the automatic protection provided by most antivirus, anti-spyware, and other anti-malware programs. This monitors computer systems for suspicious activity such as computer viruses, spyware, adware, and other malicious objects in 'real-time', in other words while data loaded into the computer's active memory: when inserting a CD, opening an email, or browsing the web, or when a file already on the computer is opened or executed.

## ***3.19 ISSUES OF CONCERN***

### **3.19.1 Unexpected renewal costs**

Some commercial antivirus software end-user license agreements include a clause that the subscription will be automatically renewed, and the purchaser's credit card automatically billed, at the renewal time without explicit approval. For example, McAfee requires users to unsubscribe at least 60 days before the expiration of the present subscription while BitDefender sends notifications to unsubscribe 30 days before the renewal. Norton antivirus also renews subscriptions automatically by default.

### **3.19.2 Rogue security applications**

Some apparent antivirus programs are actually malware masquerading as legitimate software, such as WinFixer, MS Antivirus, and Mac Defender.

### **3.19.3 Problems caused by false positives**

A "false positive" or "false alarm" is when antivirus software identifies a non-malicious file as malware. When this happens, it can cause serious problems. For example, if an antivirus program is configured to immediately delete or quarantine infected files, as is common on Microsoft Windows antivirus applications, a false positive in an essential file can render the Windows operating system or some applications unusable. Recovering from such damage to critical software infrastructure incurs technical support costs and businesses can be forced to close whilst remedial action is undertaken. For example, in May 2007 a faulty virus signature issued by Symantec mistakenly removed essential operating system files, leaving thousands of PCs unable to boot. Also in May 2007, the executable file required by Pegasus Mail on Windows was falsely detected by Norton AntiVirus as being a Trojan and it was automatically removed, preventing Pegasus Mail from running. Norton AntiVirus had falsely identified three releases of Pegasus Mail as malware, and would delete the Pegasus Mail installer file when that happened. In response to this Pegasus Mail stated:

“ On the basis that Norton/Symantec has done this for every one of the last three releases of Pegasus Mail, we can only condemn this product as too flawed to use, and recommend in the strongest terms that our users cease using it in favour of alternative, less buggy anti-

virus packages.”

- In April 2010, McAfee VirusScan detected svchost.exe, a normal Windows binary, as a virus on machines running Windows XP with Service Pack 3, causing a reboot loop and loss of all network access.
- In December 2010, a faulty update on the AVG anti-virus suite damaged 64-bit versions of Windows 7, rendering it unable to boot, due to an endless boot loop created.
- In October 2011, Microsoft Security Essentials (MSE) removed the Google Chrome web browser, rival to Microsoft's own Internet Explorer. MSE flagged Chrome as a Zbot banking trojan.
- In September 2012, Sophos' anti-virus suite identified various update-mechanisms, including its own, as malware. If it was configured to automatically delete detected files, Sophos Antivirus could render itself unable to update, required manual intervention to fix the problem.

### 3.19.4 System and interoperability related issues

Running (the real-time protection of) multiple antivirus programs concurrently can degrade performance and create conflicts. However, using a concept called multiscanning, several companies (including G Data and Microsoft) have created applications which can run multiple engines concurrently.

It is sometimes necessary to temporarily disable virus protection when installing major updates such as Windows Service Packs or updating graphics card drivers. Active antivirus protection may partially or completely prevent the installation of a major update. Anti-virus software can cause problems during the installation of an operating system upgrade, e.g. when upgrading to a newer version of Windows "in place" — without erasing the previous version of Windows. Microsoft recommends that anti-virus software be disabled to avoid conflicts with the upgrade installation process.

The functionality of a few computer programs can be hampered by active anti-virus software. For example, TrueCrypt, a disk encryption program, states on its troubleshooting page that anti-virus programs can conflict with TrueCrypt and cause it to malfunction or operate very slowly. Anti-virus software can impair the performance and stability of games running in the Steam platform.

Support issues also exist around antivirus application interoperability with common solutions like SSL VPN remote access and network access control products. These technology solutions often have policy assessment applications which require that an up to date antivirus is installed and running. If the antivirus application is not recognized by the policy assessment, whether because the antivirus application has been updated or because it is not part of the policy assessment library, the user will be unable to connect.



### 3.19.5 Effectiveness

Studies in December 2007 showed that the effectiveness of antivirus software had decreased in the previous year, particularly against unknown or zero day attacks. The computer magazine c't found that detection rates for these threats had dropped from 40-50% in 2006 to 20-30% in 2007. At that time, the only exception was the NOD32 antivirus, which managed a detection rate of 68 percent. According to the ZeuS tracker website the average detection rate for all variants of the well-known ZeuStrojan is as low as 40%.

The problem is magnified by the changing intent of virus authors. Some years ago it was obvious when a virus infection was present. The viruses of the day, written by amateurs, exhibited destructive behavior or pop-ups. Modern viruses are often written by professionals, financed by criminal organizations.

In 2008, Eva Chen, CEO of Trend Micro, stated that the anti-virus industry has over-hyped how effective its products are — and so has been misleading customers — for years.

Independent testing on all the major virus scanners consistently shows that none provide 100% virus detection. The best ones provided as high as 99.9% detection for simulated real-world situations, while the lowest provided 91.1% in tests conducted in August 2013. Many virus scanners produce false positive results as well, identifying benign files as malware.

Although methodologies may differ, some notable independent quality testing agencies include AV-Comparatives, ICSA Labs, West Coast Labs, Virus Bulletin, AV-TEST and other members of the Anti-Malware Testing Standards Organization.

### 3.19.6 New viruses

Anti-virus programs are not always effective against new viruses, even those that use non-signature-based methods that should detect new viruses. The reason for this is that the virus designers test their new viruses on the major anti-virus applications to make sure that they are not detected before releasing them into the wild.

Some new viruses, particularly ransomware, use polymorphic code to avoid detection by virus scanners. Jerome Segura, a security analyst with ParetoLogic, explained:

“ It's something that they miss a lot of the time because this type of [ransomware virus] comes from sites that use a polymorphism, which means they basically randomize the file they send you and it gets by well-known antivirus products very easily. I've seen people firsthand getting infected, having all the pop-ups and yet they have antivirus software running and it's not detecting anything. It actually can be pretty hard to get rid of, as well, and you're never really sure if it's really gone. When we see something like that usually we

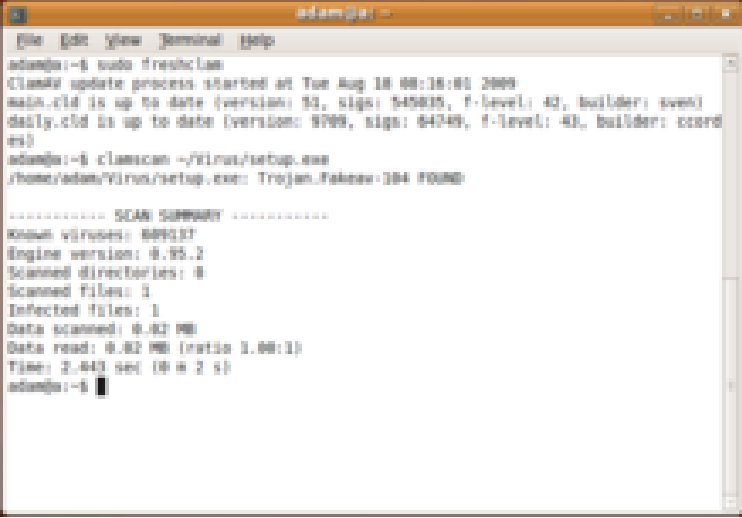
advise to reinstall the operating system or reinstall backups.“

A proof of concept virus has used the Graphics Processing Unit (GPU) to avoid detection from anti-virus software. The potential success of this involves bypassing the CPU in order to make it much harder for security researchers to analyse the inner workings of such malware.

- a. **Rootkits:** Detecting rootkits is a major challenge for anti-virus programs. Rootkits have full administrative access to the computer and are invisible to users and hidden from the list of running processes in the task manager. Rootkits can modify the inner workings of the operating system and tamper with antivirus programs.
- b. **Damaged files:** If a file has been infected by a computer virus, anti-virus software will attempt to remove the virus code from the file during disinfection, but it is not always able to restore the file to its undamaged state. In such circumstances, damaged files can only be restored from existing backups or shadow copies (this is also true for ransomware); installed software that is damaged requires re-installation (however, see System File Checker).
- c. **Firmware issues:** Active anti-virus software can interfere with a firmware update process. Any writeable firmware in the computer can be infected by malicious code. This is a major concern, as an infected BIOS could require the actual BIOS chip to be replaced to ensure the malicious code is completely removed. Anti-virus software is not effective at protecting firmware and the motherboard BIOS from infection. In 2014, security researchers discovered that USB devices contain writeable firmware which can be modified with malicious code (dubbed "BadUSB"), which anti-virus software cannot detect or prevent. The malicious code can run undetected on the computer and could even infect the operating system prior to it booting up.
- d. **Performance and other drawbacks:** Antivirus software has some drawbacks, first of which that it can impact a computer's performance. Furthermore, inexperienced users can be lulled into a false sense of security when using the computer, considering themselves to be invulnerable, and may have problems understanding the prompts and decisions that antivirus software presents them with. An incorrect decision may lead to a security breach. If the antivirus software employs heuristic detection, it must be fine-tuned to minimize misidentifying harmless software as malicious. Antivirus software itself usually runs at the highly trusted kernel level of the operating system to allow it access to all the potential malicious process and files, creating a potential avenue of attack.

### 3.19.7 Alternative solutions

The command-line virus scanner of Clam AV 0.95.2, an open source antivirus originally developed by Tomasz Kojm in 2001.



```

adam@jia: ~
┌───┴───┐
File Edit View Terminal Help
adam@jia:~$ sudo freshclam
ClamAV update process started at Tue Aug 18 08:18:01 2009
main.cvd is up to date (version: 92, sigs: 545835, F-level: 40, builder: even)
daily.cvd is up to date (version: 9709, sigs: 84749, F-level: 40, builder: cccord
es)
adam@jia:~$ clamscan -r /virus/setup.exe
./home/adam/virus/setup.exe: Trojan.Fakeav-104 FOUND

***** SCAN SUMMARY *****
Known viruses: 899337
Engine version: 0.95.2
Scanned directories: 0
Scanned files: 1
Infected files: 1
Data scanned: 0.02 MB
Data read: 0.02 MB (ratio 1.00:1)
Time: 2.643 sec (0 m 2 s)
adam@jia:~$ █

```

Figure 52: Clam AV 0.95.2<sup>75</sup>

Here running a virus signature definition update, scanning a file and identifying a Trojan. Installed antivirus solutions, running on individual computers, although the most used, is only one method of guarding against malware. Other alternative solutions are also used, including: Unified Threat Management (UTM), hardware and network firewalls, Cloud-based antivirus and on-line scanners.

### 3.19.7.1 Hardware and network firewall

Network firewalls prevent unknown programs and processes from accessing the system. However, they are not antivirus systems and make no attempt to identify or remove anything. They may protect against infection from outside the protected computer or network, and limit the activity of any malicious software which is present by blocking incoming or outgoing requests on certain TCP/IP ports. A firewall is designed to deal with broader system threats that come from network connections into the system and is not an alternative to a virus protection system.

### 3.19.7.2 Cloud antivirus

Cloud antivirus is a technology that uses lightweight agent software on the protected computer, while offloading the majority of data analysis to the provider's infrastructure. One approach to implementing cloud antivirus involves scanning suspicious files using multiple antivirus engines. This approach was proposed by an early implementation of the cloud antivirus concept called CloudAV. CloudAV was designed to send programs or documents to a network cloud where multiple antivirus and behavioural detection programs are used simultaneously in order to improve detection rates. Parallel scanning of files using potentially incompatible antivirus scanners is achieved by spawning a virtual machine per detection engine and therefore eliminating any possible issues. CloudAV can also perform "retrospective detection," whereby the cloud detection engine rescans all files in its file access history when a new threat is identified thus improving new threat detection speed. Finally, CloudAV is a solution for effective virus scanning on devices that lack the computing power to perform the scans

<sup>75</sup> .ysetruoc egam|https://en.wikipedia.org/wiki/File:ClamAV.0.95.2.png

themselves. Some examples of cloud anti-virus products are Panda Cloud Antivirus and Immunit.

### 3.19.7.3 Online scanning

Some antivirus vendors maintain websites with free online scanning capability of the entire computer, critical areas only, local disks, folders or files. Periodic online scanning is a good idea for those that run antivirus applications on their computers because those applications are frequently slow to catch threats. One of the first things that malicious software does in an attack is disable any existing antivirus software and sometimes the only way to know of an attack is by turning to an online resource that is not installed on the infected computer.

### 19.7.4 Specialist tools

The command-line rkhunter scanner, an engine to scan for Linuxrootkits. Here running the tool on Ubuntu. Virus removal tools are available to help remove stubborn infections or certain types of infection.



```

[ Rootkit Hunter version 1.3.6 ]
Checking rkhunter version
This version: 1.3.6
Latest version: 1.3.8
Update available

Performing system checks

Performing 'strings' command checks
Checking 'strings' command           [ OK ]

Performing 'shared libraries' checks
Checking for preloading variables     [ Not Found ]
Checking for preloaded libraries      [ Not Found ]
Checking LD_LIBRARY_PATH variable     [ Not Found ]

Performing file properties checks
Checking for prerequisites            [ OK ]
/bin/wash                             [ OK ]
/bin/cat                               [ OK ]
/bin/ls                                [ OK ]
/bin/ls-ls-ls                          [ OK ]
/bin/cp                                [ OK ]

```

Figure 53: rkhunter<sup>76</sup>

Examples include Trend Micro's Rootkit Buster, and rkhunter for the detection of root kits, Avira's AntiVir Removal Tool, PCTools Threat Removal Tool, and AVG's Anti-Virus Free 2011. A rescue disk that is bootable, such as a CD or USB storage device, can be used to run antivirus software outside of the installed operating system, in order to remove infections while they are dormant. A bootable antivirus disk can be useful when, for example, the installed operating system is no longer bootable or has malware that is resisting all attempts to be removed by the installed antivirus software. Examples of some of these bootable disks include the Avira AntiVir Rescue System, PCTools Alternate Operating System Scanner, and AVG Rescue CD. The AVG Rescue CD software can also be installed onto a USB storage device, that is bootable on newer computers.

## 3.20 FIREWALL

In computing, a firewall is a network security system that monitors and controls the incoming and outgoing network traffic based on predetermined security rules. A firewall typically establishes a barrier between a trusted, secure internal network and another outside network, such as the Internet, that is assumed to not be secure or trusted. Firewalls are often categorized as

<sup>76</sup> [:ysetruoc egamlhttps://en.wikipedia.org/wiki/File:Rkhunter\\_Ubuntu.png](https://en.wikipedia.org/wiki/File:Rkhunter_Ubuntu.png)

either network firewalls or host-based firewalls. Network firewalls are a software appliance running on general purpose hardware or hardware-based firewall computer appliances that filter traffic between two or more networks. Host-based firewalls provide a layer of software on one host that controls network traffic in and out of that single machine. Routers that pass data between networks contain firewall components and can often perform basic routing functions as well, Firewall appliances may also offer other functionality to the internal network they protect such as acting as a DHCP or VPN server for that network.

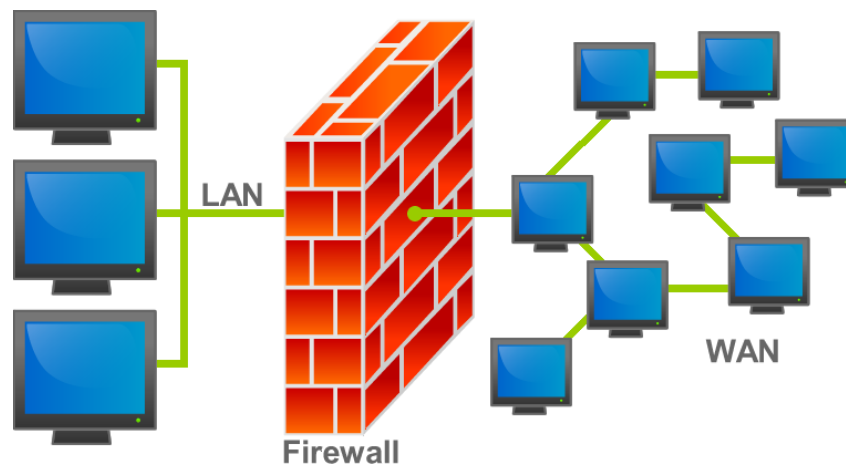


Figure 54: Firewall<sup>77</sup>

### 3.21 COMPUTER FORENSICS

Computer forensics (sometimes known as computer forensic science) is a branch of digital forensic science pertaining to evidence found in computers and digital storage media.



Figure 55: Personal storage devices<sup>78</sup>

<sup>77</sup> :ysetruoc egamlhttps://upload.wikimedia.org/wikipedia/commons/5/5b/Firewall.png

<sup>78</sup> :ysetruoc egamlhttps://upload.wikimedia.org/wikipedia/commons/8/87/PersonalStorageDevices.agr.jpg

The goal of computer forensics is to examine digital media in a forensically sound manner with the aim of identifying, preserving, recovering, analyzing and presenting facts and opinions about the digital information.

Although it is most often associated with the investigation of a wide variety of computer crime, computer forensics may also be used in civil proceedings. The discipline involves similar techniques and principles to data recovery, but with additional guidelines and practices designed to create a legal audit trail.

Evidence from computer forensics investigations is usually subjected to the same guidelines and practices of other digital evidence. It has been used in a number of high-profile cases and is becoming widely accepted as reliable within U.S. and European court systems.

In the early 1980s personal computers became more accessible to consumers, leading to their increased use in criminal activity (for example, to help commit fraud). At the same time, several new "computer crimes" were recognized (such as hacking). The discipline of computer forensics emerged during this time as a method to recover and investigate digital evidence for use in court. Since then computer crime and computer related crime has grown, and has jumped 67% between 2002 and 2003. Today it is used to investigate a wide variety of crime, including child pornography, fraud, espionage, cyberstalking, murder and rape. The discipline also features in civil proceedings as a form of information gathering (for example, Electronic discovery)

Forensic techniques and expert knowledge are used to explain the current state of a digital artifact; such as a computer system, storage medium (e.g. hard disk or CD-ROM), an electronic document (e.g. an email message or JPEG image). The scope of a forensic analysis can vary from simple information retrieval to reconstructing a series of events. In a 2002 book *Computer Forensics* authors Kruse and Heiser define computer forensics as involving "the preservation, identification, extraction, documentation and interpretation of computer data". They go on to describe the discipline as "more of an art than a science", indicating that forensic methodology is backed by flexibility and extensive domain knowledge. However, while several methods can be used to extract evidence from a given computer the strategies used by law enforcement are fairly rigid and lacking the flexibility found in the civilian world.

### **3.21.1 Use as evidence**

In court, computer forensic evidence is subject to the usual requirements for digital evidence. This requires that information be authentic, reliably obtained, and admissible. Different countries have specific guidelines and practices for evidence recovery. In the United Kingdom, examiners often follow Association of Chief Police Officers guidelines that help ensure the authenticity and integrity of evidence. While voluntary, the guidelines are widely accepted in British courts.

Computer forensics has been used as evidence in criminal law since the mid-1980s, some notable examples include:

- BTK Killer: Dennis Rader was convicted of a string of serial killings that occurred over a period of sixteen years. Towards the end of this period, Rader sent letters to the police on a floppy disk. Metadata within the documents implicated an author named "Dennis" at "Christ Lutheran Church"; this evidence helped lead to Rader's arrest.
- Joseph E. Duncan III: A spreadsheet recovered from Duncan's computer contained evidence that showed him planning his crimes. Prosecutors used this to show premeditation and secure the death penalty.
- Sharon Lopatka: Hundreds of emails on Lopatka's computer lead investigators to her killer, Robert Glass.
- Corcoran Group: This case confirmed parties' duties to preserve digital evidence when litigation has commenced or is reasonably anticipated. Hard drives were analyzed by a computer forensics expert, who could not find relevant e-mails the Defendants should have had. Though the expert found no evidence of deletion on the hard drives, evidence came out that the defendants were found to have intentionally destroyed emails, and misled and failed to disclose material facts to the plaintiffs and the court.
- Dr. Conrad Murray: Dr. Conrad Murray, the doctor of the deceased Michael Jackson, was convicted partially by digital evidence on his computer. This evidence included medical documentation showing lethal amounts of propofol.

### 3.21.2 Forensic process

Computer forensic investigations usually follow the standard digital forensic process or phases: acquisition, examination, analysis and reporting.



Figure 56: A portable Tableau write blocker attached to a Hard Drive<sup>79</sup>

Investigations are performed on static data (i.e. acquired images) rather than "live" systems. This is a change from early forensic practices where a lack of specialist tools led to investigators commonly working on live data.

<sup>79</sup> :ysetruoc egamlhttps://en.wikipedia.org/wiki/File:Portable\_forensic\_tableau.JPG

### 3.21.2.1 Techniques

A number of techniques are used during computer forensics investigations and much has been written on the many techniques used by law enforcement in particular. See, e.g., "Defending Child Pornography Cases".

### 3.21.2.2 Cross-drive analysis

A forensic technique that correlates information found on multiple hard drives. The process, still being researched, can be used to identify social networks and to perform anomaly detection.

### 3.21.2.3 Live analysis

The examination of computers from within the operating system using custom forensics or existing sysadmin tools to extract evidence. The practice is useful when dealing with Encrypting File Systems, for example, where the encryption keys may be collected and, in some instances, the logical hard drive volume may be imaged (known as a live acquisition) before the computer is shut down.

### 3.21.2.3 Deleted files

A common technique used in computer forensics is the recovery of deleted files. Modern forensic software have their own tools for recovering or carving out deleted data. Most operating systems and file systems do not always erase physical file data, allowing investigators to reconstruct it from the physical disk sectors. File carving involves searching for known file headers within the disk image and reconstructing deleted materials.

### 3.21.2.4 Volatile data

When seizing evidence, if the machine is still active, any information stored solely in RAM that is not recovered before powering down may be lost. One application of "live analysis" is to recover RAM data (for example, using Microsoft's COFEE tool, windd, WindowsSCOPE) prior to removing an exhibit. CaptureGUARD Gateway bypasses Windows login for locked computers, allowing for the analysis and acquisition of physical memory on a locked computer. RAM can be analyzed for prior content after power loss, because the electrical charge stored in the memory cells takes time to dissipate, an effect exploited by the cold boot attack. The length of time that data is recoverable is increased by low temperatures and higher cell voltages. Holding unpowered RAM below  $-60^{\circ}\text{C}$  helps preserve residual data by an order of magnitude, improving the chances of successful recovery. However, it can be impractical to do this during a field examination.

Some of the tools needed to extract volatile data, however, require that a computer be in a forensic lab, both to maintain a legitimate chain of evidence, and to facilitate work on the machine. If necessary, law enforcement applies techniques to move a live, running desktop computer. These include a mouse jiggler, which moves the mouse rapidly in small movements and prevents the computer from going to sleep accidentally. Usually, an uninterruptible power supply (UPS) provides power during transit.



However, one of the easiest ways to capture data is by actually saving the RAM data to disk. Various file systems that have journaling features such as NTFS and ReiserFS keep a large portion of the RAM data on the main storage media during operation, and these page files can be reassembled to reconstruct what was in RAM at that time.

#### **3.21.2.4 Analysis tools**

A number of open source and commercial tools exist for computer forensics investigation. Typical forensic analysis includes a manual review of material on the media, reviewing the Windows registry for suspect information, discovering and cracking passwords, keyword searches for topics related to the crime, and extracting e-mail and pictures for review.

#### **3.21.2.5 Stochastic forensics**

A method which uses stochastic properties of the computer system to investigate activities lacking digital artifacts. Its chief use is to investigate data theft.

### **3.22 STEGANOGRAPHY**

One of the techniques used to hide data is via steganography, the process of hiding data inside of a picture or digital image. An example would be to hide pornographic images of children or other information that a given criminal does not want to have discovered. Computer forensics professionals can fight this by looking at the hash of the file and comparing it to the original image (if available.) While the image appears exactly the same, the hash changes as the data changes. In Forensic examination, Steganalysis is used to get the details of Steganographic contents.

- 21 CFR 11
- Blind signature
- Detached signature
- Digital certificate
- Digital signature in Estonia
- Digital signatures and law
- Electronic lab notebook
- Electronic signature
- eSign (India)
- GNU Privacy Guard
- Global Trust Center
- PAdES
- Public key infrastructure
- Server-based signatures
- Electronic commerce
- Very Large Business Applications
- Digital economy
- Types of E-commerce
- Shopping cart software

### **3.23 SUMMARY**

1. Modern electronic commerce typically uses the World Wide Web for at least one part of the transaction's life cycle, although it may also use other technologies such as e-mail.
2. E-Business systems naturally have greater security risks than traditional business systems, therefore it is important for e-business systems to be fully protected against these risks.
3. E-business transactions pose greater challenges for establishing authenticity due to the ease with which electronic information may be altered and copied.
4. A business must have assurance that the receiving party or purchaser cannot deny that a transaction has occurred, and this means having sufficient evidence to prove the transaction.
5. When certain electronic resources and information is limited to only a few authorized individuals, a business and its customers must have the assurance that no one else can access the systems or information.
6. When it comes to security solutions, sustainable electronic business requires support for data integrity, strong authentication, and privacy.
7. A firewall is used to restrict access to private networks, as well as public networks that a company may use.
8. Encryption, which is actually a part of cryptography, involves transforming texts or messages into a code which is unreadable.
9. In order to use a digital signature, one must use a combination of cryptography and a message digest.
10. Authentication is the process of determining whether someone or something is, in fact, who or what it is declared to be.
11. Authorization is the process of giving someone permission to do or have something. In multi-user computer systems, a system administrator defines for the system which users are allowed access to the system and what privileges of use (such as access to which file directories, hours of access, amount of allocated storage space, and so forth).
12. Smart cards are the credit card-sized plastic cards that house an embedded integrated circuit.
13. Secure Electronic Transaction (SET) was a communications protocol standard for securing credit card transactions over insecure networks, specifically, the Internet.
14. A digital signature is a mathematical scheme for demonstrating the authenticity of a digital message or documents.
15. Digital signatures cryptographically bind an electronic identity to an electronic document and the digital signature cannot be copied to another document.

### **3.24 CHECK YOUR PROGRESS**

- 1 EDI stands for \_\_\_\_\_.

- 2 \_\_\_\_\_ is the extent to which businesses makes personal information available to other businesses and individuals.
- 3 VPN stands for \_\_\_\_\_.
- 4 \_\_\_\_\_ deals with the existence of proof in a transaction.
- 5 One way to address non-repudiation is using \_\_\_\_\_ .
- 6 UPS stands for \_\_\_\_\_.
- 7 The \_\_\_\_\_ also has the ability to log attempts into the network and provide warnings as it is happening.
- 8 The public one is used for \_\_\_\_\_ , and the private for \_\_\_\_\_.
- 9 A \_\_\_\_\_ is used to give the document a unique value.
- 10 \_\_\_\_\_ is a scheme established and maintained, whereby users are properly, consistently, effectively and efficiently identified before systems are accessed.
- 11 \_\_\_\_\_ is verification of the identity of the entity requesting access to a system.
- 12 \_\_\_\_\_ authentication requires that the user uses a user id, password combined with any other form of authentication method as smartcard or biometric.
- 13 \_\_\_\_\_ is a biometric authentic technique that uses data related to the unique facial features of a user.
- 14 \_\_\_\_\_ is a form of peer-to-peer protocol (PPP) mechanism used by an authenticator to authenticate a peer.
- 15 Digital signatures employ \_\_\_\_\_ cryptography.

### **3.25 ANSWERS TO CHECK YOUR PROGRESS**

1. electronic data interchange
2. Confidentiality
3. virtual private network
4. Non- repudiation
5. digital signatures
6. Uninterrupted Power Supply
7. Firewall
8. Encryption, decryption
9. message digest
10. Identification
11. Authentication
12. Multi-factor
13. Facial recognition
14. CHAP authentication
15. asymmetric

### **3.26 MODEL QUESTIONS**

1. What is e-commerce?

2. What is a business model?
3. Explain the revenue model of a e-commerce company?
4. Discuss the concerns that must be addressed before starting an e-commerce company.
5. Define data integrity.
6. What are the different techniques to address the problem of access control?
7. What is a digital certificate?
8. What is the difference between identification, authentication and authorization?
9. What are the different types of ecommerce authentication?
10. What is a security token?
11. What are the different types of biometric authentication?
12. What is Hand Geometry Authentication?
13. What is Secure Electronic Transaction?
14. Explain the working of a digital signature.
15. Compare digital signatures with ink on paper signatures.
16. What is an antivirus?
17. What is a firewall?

## UNIT IV: ETHICAL ASPECT OF INFORMATION SECURITY

### 4.1 LEARNING OBJECTIVES

A student after going through this unit will be able to understand concepts of:

- Ethical aspects involved in Information Security
- Information Privacy and Ethics
- Privacy issues involved in Modern Data Management
- Tactics for ensuring proper information security
- E-mail Security
- Physical Security
- Web Security

### 4.2 INTRODUCTION

This unit will review ethical aspects of computer and information security and privacy. Ethics is a field of study that is concerned with distinguishing right from wrong, and good from bad. It analyzes the morality of human behaviors, policies, laws and social structures. Ethicists attempt to justify their moral judgments by reference to ethical principles of theories that attempt to capture our moral intuitions about what is right and wrong. The two theoretical approaches that are most common in ethics are consequentialism and deontology. Consequentialist approaches assume that actions are wrong to the extent that they have bad consequences, whereas deontological approaches assume that people have moral duties that exist independently of any good or bad consequences that their actions may have. Ethical principles often inform legislation, but it is recognized in ethics that legislation cannot function as a substitute for morality. It is for this reason that individuals and corporations are always required to consider not only the legality but also the morality of their actions. Ethical analysis of security and privacy issues in information technology primarily takes place in computer ethics which emerged in the 1980s as a field. Computer ethics analyzes moral responsibilities of computer professionals and computer users and ethical issues in public policy for information technology development and use. It asks such questions as:

- Is it wrong for corporations to read their employee's e-mail?
- Is it morally permissible for computer users to copy copyrighted software?
- Should people be free to put controversial or pornographic content online without censorship?

Ethical issues and questions like these require moral or ethical analysis: analysis in which the moral dilemmas contained in these issues are clarified and solutions are proposed for them. Moral analysis aims to get clear on the facts and values in such cases, and to find a balance between the various values, rights and interests that are at stake and to propose or evaluate policies and courses of action.

### **4.3 COMPUTER SECURITY AND ETHICS**

We will now turn to ethical issues in computer and information security. In this section, the moral importance of computer security will be assessed, as well as the relation between computer security and national security.

#### **4.3.1 The Moral Importance of Computer Security**

Computer security is a field of computer science concerned with the application of security features to computer systems to provide protection against the unauthorized disclosure, manipulation, or deletion of information, and against denial of service. The condition resulting from these efforts is also called computer security. The aim of computer security professionals is to attain protection of valuable information and system resources. A distinction can be made between the security of system resources and the security of information or data. The first may be called system security, and the second information security or data security. System security is the protection of the hardware and software of a computer system against malicious programs that sabotage system resources. Information security is the protection of data that resides on disk drives on computer systems or is transmitted between systems. Information security is customarily defined as concerned with the protection of three aspects of data: their confidentiality, integrity and availability.

#### **4.3.2 How does computer security pose ethical issues?**

As explained earlier, ethics is mostly concerned with rights, harms and interests. We may therefore answer this question by exploring the relation between computer security and rights, harms and interests.

- What morally important benefits can computer security bring?
- What morally important harms or violations of moral rights can result from a lack of computer security?
- Can computer security also cause harms or violate rights instead of preventing and protecting them?

A first and perhaps most obvious harm that can occur from breaches of computer security is economic harm. When system security is undermined, valuable hardware and software may be damaged or corrupted and service may become unavailable, resulting in losses of time, money and resources. Breaches of information security may come at an even higher economic cost. Valuable data may be lost or corrupted that is worth much more than the hardware on which it is stored, and this may cause severe economic losses. Stored data may also have personal, cultural or social value, as opposed to economic value, that can be lost when data is corrupted or lost. Any type of loss of system or data security is moreover likely to cause some amount of psychological or emotional harm.

Breaches of computer security may even cause grave harms like injury and death. This may occur in so-called safety-critical systems, which are computer systems with a component or real-time control that can have a direct life-threatening impact. Examples are computer systems in

nuclear reactor control, aircraft and air traffic control, missile systems and medical-treatment systems. The corruption of certain other types of systems may also have life-threatening consequences in a more indirect way.

These may include systems that are used for design, monitoring, diagnosis or decision-making, for instance systems used for bridge design or medical diagnosis. Compromises of the confidentiality of information may cause additional harms and rights violations. Third parties may compromise the confidentiality of information by accessing, copying and disseminating it. Such actions may, first of all, violate property rights, including intellectual property rights, which are rights to own and use intellectual creations such as artistic or literary works and industrial design. The information may be exclusively owned by someone who has the right to determine who can access and use the information, and this right can be violated.

Second, compromises of confidentiality may violate privacy rights. This occurs when information that is accessed includes information about persons that is considered to be private. In addition to violations of property and privacy rights, breaches of confidentiality may also cause a variety of other harms resulting from the dissemination and use of confidential information. For instance, dissemination of internal memos of a firm damages its reputation, and compromises of the confidentiality of online credit card transactions undermines trust in the security of online financial transactions and harms e-banking and e-commerce activity.

Compromises of the availability of information can, when they are prolonged or intentional, violate freedom rights, specifically rights to freedom of information and free speech. Freedom of information is the right to access and use public information. Jeroen van den Hoven has argued that access to information has become a moral right of citizens in the information age, because information has become a primary social good: a major resource necessary for people to be successful in society. Shutting down vital information services could violate this right to information. In addition, computer networks have become important as a medium for speech. Websites, e-mail, bulletin boards, and other services are widely used to spread messages and communicate with others. When access to such services is blocked, for instance through denial of service attacks or hijackings of websites, such acts are properly classified as violations of free speech. Computer security measures normally prevent harms and protect rights, but they can also cause harm and violate rights. Notably, security measures may be so protective of information and system resources that they discourage or prevent stakeholders from accessing information or using services. Security measures may also be discriminatory: they may wrongly exclude certain classes of users from using a system, or may wrongly privilege certain classes of users over others.

### **4.3.3 Computer Security and National Security**

Developments in computer security have been greatly influenced by the September 11, 2001 terrorist attacks in the United States and their aftermath. In response to these attacks, national

security has become a major policy concern of Western nations. National security is the maintenance of the integrity and survival of the nation-state and its institutions by taking measures to defend it from threats, particularly threats from the outside. Many new laws, directives and programs protective of national security have come into place in Western nations after 9/11, including the creation in the U.S. of an entire Department of Homeland Security. The major emphasis in these initiatives is the protection of state interests against terrorist attacks. Information technology has acquired a dual role in this quest for national security. First of all, computer security has become a major priority, particularly the protection of critical information infrastructure from external threats. Government computers, but also other public and private infrastructure, including the Internet and telephone network, have been subjected to stepped-up security measures. Secondly, governments have attempted to gain more control over public and private information infrastructures. They have done this through wiretapping and data interception, by requiring Internet providers and telephone companies to store phone and e-mail communications records and make them available to law enforcement officials, by attempting to outlaw certain forms of encryption, or even through attempts to require companies to reengineer Internet so that eavesdropping by the government is made easier. Paradoxically, these efforts by governments to gain more control over information also lessen certain forms of security: they make computers less secure from access by government agencies.

Philosopher Helen Nissenbaum has argued that the current concern for national security has resulted in a new conception of computer security next to the classical one. The classical or ordinary conception of computer security is the one used by the technical community and defines computer security in terms of systems security and integrity, availability and confidentiality of data. Nissenbaum calls this technical computer security. The other, which she calls cybersecurity, involves the protection of information infrastructure against threats to national interests. Such threats have come to be defined more broadly than terrorism, and have nowadays come to include all kinds of threats to public order, including internet crime, online child pornography, computer viruses, and racist and hate-inducing websites. At the heart of cybersecurity, however, are concerns for national security, and especially the state's vulnerability to terrorist attacks.

Nissenbaum emphasizes that technical computer security and cybersecurity have different conceptions of the aims of computer security and the measures that need to be taken. Technical computer security aims to protect the private interests of individuals and organizations, specifically owners and users of computer systems and data. Cybersecurity aims to protect the interests of the nation-state and conceives of computer security as a component of national security. Technical computer security measures mostly protect computer systems from outside attacks. Cybersecurity initiatives include such protective measures as well, but in addition include measures to gain access to computer systems and control information. The two conceptions of security come into conflict when they recommend



opposite measures. For instance, cyber-security may require computers system to be opened up to remote government inspection or may require government access to websites to shut them down, while technical computer security may prohibit such actions. The different interests of technical computer security and cybersecurity can in this way create moral dilemmas: should priority be given to state interests or to the interests and rights of private parties? This points to the larger dilemma of how to balance national security interests against civil rights after 9/11.

#### ***4.4 ETHICAL ISSUES IN COMPUTER SECURITY***

In this section, ethical aspects of specific practices in relation to computer security will be analyzed. Section 4.4.1 and 4.4.2 will focus on practices that undermine computer security: hacking, computer crime, cyber terrorism and information warfare. Section 3.3 will consider the moral responsibilities of information security professionals.

##### **4.4.1 Hacking and Computer Crime**

A large part of computer security is concerned with the protection of computer resources and data against unauthorized, intentional break-ins or disruptions. Such actions are often called hacking. Hacking, is the use of computer skills to gain unauthorized access to computer resources. Hackers are highly skilled computer users that use their talents to gain such access, and often form communities or networks with other hackers to share knowledge and data. Hacking is often also defined, more negatively, as the gaining of such unauthorized access for malicious purposes: to steal information and software or to corrupt data or disrupt system operations. Self-identified hackers, however, make a distinction between non-malicious break-ins, which they describe as hacking, and malicious and disruptive break-ins, which they call cracking. Self-identified hackers often justify their hacking activities by arguing that they cause no real harm and instead have a positive impact. The positive impact of hacking, they argue, is that it frees data to the benefit of all, and improves systems and software by exposing security holes. The reconsiderations are part of what has been called the hacker ethic or hacker code of ethics, which is a set of (usually implicit) principles that guide the activity of many hackers. Such principles include convictions that information should be free, that access to computers should be unlimited and total, and that activities in cyberspace cannot do harm in the real world. Various professionals have argued that many principles of the hacker ethic cannot be sustained. The belief that information should be free runs counter to the very notion of intellectual property, and would imply that creators of information would have no right to keep it to themselves and have no opportunity to make a profit from it. It would moreover fundamentally undermine privacy, and would undermine the integrity and accuracy of information, as information could be modified and changed at will by anyone who would access it. A school of thought, that the helpfulness of hacking in pointing to security weaknesses may not outweigh the harm it does, and that activities in cyberspace can do harm in the real world.

Both hacking and cracking tend to be unlawful, and may therefore be classified as a form of computer crime, or cybercrime, as it has also been called. There are many varieties of computer crime, and not all of them compromise computer security. There are two major types of cybercrime that compromise computer security:

- cybertrespass, which is defined as the use of information technology to gain unauthorized access to computer systems or password-protected websites, and
  - cybervandalism, which is the use of information technology to unleash programs that disrupt the operations of computer networks or corrupt data.
- Another type of cybercrime that sometimes includes breaches of computer security, cyberpiracy.

Cyberpiracy, also called software piracy, is the use of information technology to reproduce copies of proprietary software or information or to distribute such data across a computer network. Cyberpiracy is much more widespread than cybervandalism or cybertrespass, because it does not require extensive computer skills and many computer users find it morally permissible to make copies of copyrighted software and data. Cyberpiracy involves breaches in computer security when it includes the cracking of copyright protections. Another type of cybercrime that sometimes involves breaches of computer security is computer fraud, which is deception for personal gain in online business transactions by assuming a false online identity or by altering or misrepresenting data. Computer fraud may depend on acts of cyber trespass to obtain passwords, digital identities, or other transaction or access codes, and acts of cybervandalism involving the modification of data. Other types of cybercrime, such as the online distribution of child pornography or online harassment and libel, usually do not involve breaches of computer security.

#### **4.4.2 Cyberterrorism and Information Warfare**

A recent concern in computer and national security has been the possibility of cyberterrorism, which is defined by Herman Tavani as the execution of “politically motivated hacking operations intended to cause grave harm, that is, resulting in either loss of life or severe economic loss, or both”. The possibility of major attacks on information infrastructure, intending to debilitate or compromise this infrastructure and harm economic, industrial or social structures dependent on it, has become a major concern since the 9/11 attacks. Such attacks could be both foreign and domestic. Controversy exists on the proper scope of “cyberterrorism”. Where should the boundaries be drawn between cyberterrorism, cybercrime, and cybervandalism? Should a teenager who releases a dangerous virus that turns out to cause major harm to government computers be persecuted as a cyberterrorist? Are politically motivated hijackings of the homepages of major organizations acts of cyberterrorism? A distinction between cyberterrorism and other kinds of cyberattacks may be found in its political nature: cyberterrorism consists of politically motivated operations that aim to cause harm. Yet, Mark Mainon and Abby Goodrum have argued that not all politically motivated cyberattacks should be called cyberterrorism. They distinguish cyberterrorism from hacktivism, which are hacking operations against an internet site or server with the intent to

disrupt normal operations but without the intent to cause serious damage. Hacktivists may make use of e-mail bombs, low-grade viruses, and temporary homepage hijackings. They are politically motivated hackers who engage in a form of electronic political activism that should be distinguished from terrorism. Information warfare is an extension of ordinary warfare in which combatants use information and attacks on information and information systems as tools of warfare. Information warfare may include the use of information media to spread propaganda, the disruption, jamming or hijacking of communication infrastructure or propaganda feeds of the enemy, and hacking into computer systems that control vital infrastructure (e.g., oil and gas pipelines, electric power grids, or railway infrastructure).

#### **4.4.3 Moral Responsibilities of Information Security Professionals**

Information security (IS) professionals are individuals whose job it is to maintain system and information security. By standing of their profession, they have a professional responsibility to assure the correctness, reliability, availability, safety and security of all aspects of information and information systems. The discussion in the above sections makes clear that this responsibility has a moral dimension: professional activities in computer security may protect people from morally important harms but could also cause such harms, and may either protect or violate people's moral rights. In case of safety-critical systems, the decisions of information security professionals may even be a matter of life or death. That IS professionals have moral responsibilities as part of their profession is reflected in codes of ethics used by various organizations for computer and information security. These codes of ethics rarely go into detail, however, on the moral responsibilities of IS professionals in specific situations. For instance, the code of ethics of the Information Systems Security Association (ISSA), an international organization of information security professionals and practitioners, only states that members should "perform all professional activities and duties in accordance with all applicable laws and the highest ethical principles" but does not go on to specify what these ethical principles are or how they should be applied and balanced against each other in specific situations. For IS professionals, as well as for other computer professionals who have a responsibility for computer security, a code of ethics clearly is not enough. To appreciate the moral dimension of their work, and to cope with moral dilemmas in it, they require training in information security ethics. Such training helps professionals to get clear about interests, rights, and moral values that are at stake in computer security, to recognize ethical questions and dilemmas in their work, and to balance different moral principles in resolving such ethical issues.

#### **4.5 INFORMATION PRIVACY AND ETHICS**

We will now turn to issues of privacy in modern data management. In this section, it will be considered what privacy is, why it is important and how it is impacted by information technology. Section 4.6 will then consider major privacy issues in modern data management.

### **4.5.1 What is Privacy and Why is It Important?**

In Western societies, a broad recognition exists of a right to personal privacy. The right to privacy was first defended by the American justices Samuel Warren and Louis Brandeis, who defined privacy as “the right to be let alone”. Privacy is a notion that is difficult to define, and many more precise definitions have since been presented. Often, the right to privacy is defined as the right of individuals to control access or interference by others into their private affairs. Philosopher Ferdinand Schoeman has defined it thus: “A person has privacy to the extent that others have limited access to information about him, limited access to the intimacies of his life, or limited access to his thoughts or his body.” Schoeman’s definition shows that the concept of privacy does not only apply to the processing of personal information. It also applies to the observation of and interference with human behaviors and relations, the human body, and one’s home and personal belongings. Privacy is held to be valuable for several reasons. Most often, it is held to be important because it is believed to protect individuals from all kinds of external threats, such as defamation, ridicule, harassment, manipulation, blackmail, theft, subordination, and exclusion. James Moor has summed this up by claiming that privacy is an articulation of the core value of security, meant to protect people from all kinds of harm done by others. It has also been argued that privacy is a necessary condition for autonomy: without privacy, people could not experiment in life and develop their own personality and own thoughts, because they would constantly be subjected to the judgment of others. The right to privacy has also been claimed to protect other rights, such as abortion rights and the right to sexual expression. Privacy moreover has been claimed to have social value in addition to individual value. It has, for instance, been held to be essential for maintaining democracy.

The right to privacy is not normally held to be absolute: it must be balanced against other rights and interests, such as the maintenance of public order and national security. Privacy rights may also vary in different contexts. There is, for example, a lesser expectation of privacy in the workplace or in the public sphere than there is at home. An important principle used in privacy protection in Western nations is that of informed consent: it is often held that citizens should be informed about how organizations plan to store, use or exchange their personal data, and that they should be asked for their consent. People can then voluntarily give up their privacy if they choose.

### **4.5.2 Information Technology and Privacy**

Privacy is a value in modern societies that corresponds with the ideal of the autonomous individual who is free to act and decide his own destiny. Yet, modern societies are also characterized by surveillance, a practice that tends to undermine privacy. Surveillance is the systematic observation of (groups of) people for specific purposes, usually with the aim of exerting some form of influence over them. Sociologist David Lyon has argued that surveillance has always been an important part of modern societies. The state engages in surveillance to protect national security and to fight crime, and the modern corporation engages

in surveillance in the workplace to retain control over the workforce. Computerization from the 1960s onward has intensified surveillance by increasing its scale, ease and speed. Surveillance is partially delegated to computers that help in collecting, processing and exchanging data. Computers have not only changed the scale and speed of surveillance, they have also made a new kind of surveillance possible: dataveillance, which is the large-scale, computerized collection and processing of personal data in order to monitor people's actions and communications. More and more, information technology is not just used to record and process static information about individuals, but to record and process their actions and communications. New detection technologies like smart closed-circuit television (CCTV), biometrics and Intelligent User Interfaces, and new data processing techniques like data mining further exacerbate this trend. As Lyon has argued, the ease with which surveillance now takes place has made it a generalized activity that is routinely performed in all kinds of settings by different kinds of organizations. Corporations, for instance, have extended surveillance from the workplace to their customers (consumer surveillance). In addition, the 9/11 terrorist attacks have drastically expanded surveillance activities by the state. Many privacy disputes in today's society result from tensions between people's right to privacy and state and corporate interests in surveillance. In the information society, privacy protection is realized through all kinds of information privacy laws, policies and directives, or data protection policies, as they are often called in Europe. These policies regulate the harvesting, processing, usage, storage and exchange of personal data. They are often overtaken, however, by new developments in technology. However, privacy protection has also become a concern in the design and development of information technology. Information privacy has also become a major topic of academic study. Studies of information privacy attempt to balance privacy rights against other rights and interests, and try to determine privacy rights in specific contexts and for specific practices. Specialized topics include workplace privacy, medical privacy, genetic privacy, Internet privacy, and privacy in public.

## ***4.6 PRIVACY ISSUES IN MODERN DATA MANAGEMENT***

### **4.6.1 Internet Privacy**

The Internet raises two kinds of privacy issues. First, the posting and aggregation of personal information on Internet websites sometimes violates privacy. Websites on the Internet contain all sorts of personal information that is made publicly available, often without the bearer's explicit consent. They may contain, for instance, one's phone number and address, archived bulletin board messages from years past, information about one's membership of organizations, online magazines and newspapers in which one is mentioned, online databases with public records, pictures and video clips featuring oneself, etc. Using search engines, this information can easily be located and be used to create elaborate composite records about persons. Should there be limits to this? When should someone's consent be asked when his personal information is posted on the web, or when such information is used for specific purposes?

A second type of privacy issue involves the online monitoring of internet users. Their connection to the internet may be used by third parties to collect information about them, in a way that is often invisible to them. Online privacy risks include cookies (small data packets placed by servers on one's computer for user authentication, user tracking, and maintaining user-specific information), profiling or tracking (recording the browsing behavior of users), and spyware (computer programs that maliciously collect information from a user's computer system or about a user's browser behavior and send this information over the internet to a third party). In addition, private e-mail and data traffic may be intercepted at various points, for instance by employers, internet service providers, and government agencies. When do such actions violate privacy, and what should be done to protect internet privacy?

#### **4.6.2 Record Merging and Matching and Data Mining**

It frequently happens that different databases with personal information are combined to produce new data structures. Such combinations may be made in two ways. First, the records in two databases may be merged to produce new composite records. For instance, a credit card company may request information about its prospective customers from various databases (e.g., financial, medical, insurance), which are then combined into one large record. This combined record is clearly much more privacy-sensitive than the records that compose it, as the combined record may generate perceptions and suggest actions that would not have resulted from any of the individual records that make it up. Second, records in databases may be matched. Computer matching is the cross-checking in two or more unrelated databases for information that fits a certain profile in order to produce matching records or "hits". Computer matching is used often by government agencies to detect possible instances of fraud or other crimes. For instance, ownership records of homes or motorized vehicles may be matched with records of welfare recipients to detect possible instances of welfare fraud. Computer matching has raised privacy concerns because it is normally done without the consent of the bearers of personal information that are involved. Moreover, matches rarely prove facts about persons but rather generate suspicions that require further investigation. In this way, record matching could promote stereotyping and lead to intrusive investigations. Data Mining is a technique that is usually defined over a single database. It is the process of automatically searching large volumes of data for patterns, using techniques like statistical analysis, machine learning and pattern recognition. When data mining takes place in databases containing personal information, the new information thus gained may be privacy sensitive or confidential even when the old information is not. It may for instance uncover patterns of behavior of persons that were not previously visible. Data mining may also be used to stereotype whole categories of individuals. For instance, a credit card company may use data mining on its customer database to discover that certain zip codes correlate strongly with loan defaults. It may then decide not to extend credit anymore to customers with these zip codes. In summary, data mining may violate individual privacy and may be used to stereotype whole categories of individuals. Ethical policies are needed to prevent this from happening.

### 4.6.3 Privacy in Public

It is sometimes believed that privacy is a right that people have when they are in private places like homes, private clubs and restrooms, but that is minimized or forfeited as soon as they enter public space. When you walk in public streets or are on the road with your car, it is sometimes believed, you may retain the right not to be seized and searched without probable cause, but your appearance and behavior may be freely observed, surveilled and registered. Many privacy scholars, however, have argued that this position is not wholly tenable, and that people have privacy rights in public areas that are incompatible with certain registration and surveillance practices. The problem of privacy in public applies to the tracking, recording, and surveillance of public appearances, movements and behaviors by individuals and their vehicles. Techniques that are used for this including video surveillance (CCTV), including smart CCTV for facial recognition, infrared cameras, satellite surveillance, GPS tracking, RFID tagging, electronic checkpoints, mobile phone tracking, audio bugging, and ambient intelligence techniques. Does the use of these techniques violate privacy even when they are used in public places? The problem of privacy in public also applies to publicly available information on the Internet. Does the fact that personal information is available on a public forum make it all right to harvest this information, aggregate it and use it for specific purposes?

Helen Nissenbaum has argued in an influential paper that surveillance in public places that involves the electronic collection, storage and analysis of information on a large scale often amounts to a violation of personal privacy. She argues that people often experience such surveillance as an invasion of their privacy if they are properly informed about it, and that such electronic harvesting of information is very different from ordinary observation, because it shifts information from one context to another and frequently involves record merging and matching and data mining. She concludes that surveillance in public places violates privacy whenever it violates contextual integrity: the trust that people have that acquired information appropriate to one context will not be used in other contexts for which it was not intended.

### 4.6.4 Biometric Identification

Biometrics is the identification or verification of someone's identity on the basis of physiological or behavioral characteristics. Biometric technologies provide a reliable method of access control and personal identification for governments and organizations. However, biometrics has also raised privacy concerns. Widespread use of biometrics would have the undesirable effect of eliminating anonymity and pseudonymity in most daily transactions, because people would leave unique traces everywhere they go. Moreover, the biometric monitoring of movements and actions gives the monitoring organization insight into a person's behaviors which may be used against that person's interests. In addition, many people find biometrics distasteful, because it involves the recording of unique and intimate aspects of (rather than about) a person, and because biometric identification procedures are sometimes invasive of bodily privacy. The challenge for biometrics is therefore to develop techniques and policies that are optimally protective of personal privacy.

### **4.6.5 Ubiquitous Computing and Ambient Intelligence**

Ubiquitous Computing is an approach in information technology that aims to move computers away from the single workstation and embed microprocessors into everyday working and living environments in an invisible and unobtrusive way. Ambient Intelligence is an advanced form of ubiquitous computing that incorporates wireless communication and Intelligent User Interfaces, which are interfaces that use sensors and intelligent algorithms for profiling (recording and adapting to user behavior patterns) and context awareness (adapting to different situations). In Ambient Intelligence environments, people are surrounded with possibly hundreds of intelligent, networked computers that are aware of their presence, personality and needs, and perform actions or provide information based on their perceived needs. Marc Langheinrich has claimed that ubiquitous computing has four unique properties that are potentially threatening to privacy:

- 1 ubiquity;
- 2 invisibility
- 3 sensing;
- 4 memory amplification (the continuous recording of people's actions to create searchable logs of their past). Ambient Intelligence adds two properties to this list:
- 5 user profiling; and
- 6 connectedness (wireless communication between smart objects) .

These unique features of the two technologies make the protection of privacy in them a major challenge. As critics have argued, ubiquitous computing and ambient intelligence have the ability to create a Big Brother society in which every human activity is recorded and smart devices probe people's actions, intentions and thoughts. The distinction between the private and the public sphere may be obliterated as dozens of smart devices record activity in one's home or car and connect to corporate or government computers elsewhere. Major privacy safeguards will be needed to avoid such scenarios.

### ***4.7 TACTICS TO ENSURE COMPUTER SECURITY AND MAINTAIN PRIVACY***

These tactics guides cover the basics of digital security and recommend tools you can use

- Protect your device from malware and hackers :Prevent worms, viruses and trojans
- Protect your information from physical threats : Ensure your workplace and devices are secure
- Create and maintain secure passwords : Learn to manage strong passwords
- Protect the sensitive files on your computer : Learn to encrypt data and files
- Recover from information loss : Back up your devices and data
- Destroy sensitive information : Delete data permanently
- Keep your online communication private : Encrypted chat and email
- Remain anonymous and bypass censorship on the Internet : Using Tor and VPNs



- Protect yourself and your data when using social networking sites : Using Facebook, Twitter and Flickr safely
- Use mobile phones as securely as possible : Staying safe when using cellphones
- Use smartphones as securely as possible : Android and iPhone safety

## **4.8 SUMMARY**

Privacy is a moral right of individuals that is frequently and increasingly at issue when information systems are used. It was explained in this essay why privacy is important and how it is impacted by information technology, and various ethical issues in information privacy were reviewed. Computer security is not itself a moral right or moral value, but it has been argued that maintaining computer security may be morally necessary to protect correlated rights and interests: privacy rights, property rights, freedom rights, human life and health and national security. It was argued that computer security can also work to undermine rights. Ethical analysis of privacy and security issues in computing can help computer professionals and users recognize and resolve moral dilemmas and can yield ethical policies and guidelines for the use of information technology. In addition, it has been recognized in computer ethics that not only the use of information systems requires moral reflection, but also their design, as system designs reflect moral values and involve moral choices. A system can for example be designed to protect privacy, but it can also be designed to give free access to personal information to third parties. This fact is taken up in value-sensitive design, an approach to the design of information systems that attempts to account for values in a principled fashion. Ideally, ethical reflection on information technology should not wait until products hit the market, but should be built in from the beginning by making it part of the design process. Digital world poses great danger to privacy and security, however it can be tackled to a great extent by adhering to disciplined approach as prescribed. Freeware and Open Source Softwares are of great help in achieving Information Security to a fairly great extent.

## **4.9 CHECK YOUR PROGRESS**

1. The two theoretical approaches that are most common in ethics are \_\_\_\_\_ and \_\_\_\_\_.
2. Ethical principles often inform legislation, but it is recognized in ethics that legislation cannot function as a substitute for \_\_\_\_\_ .
3. \_\_\_\_\_ is the protection of data that resides on disk drives on computer systems or is transmitted between systems.
4. \_\_\_\_\_ is the use of computer skills to gain unauthorized access to computer resources.
5. \_\_\_\_\_ is the use of information technology to reproduce copies of proprietary software or information or to distribute such data across a computer network.
6. \_\_\_\_\_ is defined as politically motivated hacking operations intended to cause grave harm, that is, resulting in either loss of life or severe economic loss, or both.

7. \_\_\_\_\_ is the large-scale, computerized collection and processing of personal data in order to monitor people's actions and communications.
8. \_\_\_\_\_ is the identification or verification of someone's identity on the basis of physiological or behavioral characteristics.

#### ***4.10 ANSWERS TO CHECK YOUR PROGRESS***

1. Consequentialism, deontology.
2. Morality
3. Information security
4. Hacking
5. Cyberpiracy
6. Cyberterrorism
7. Dataveillance
8. Biometrics

#### ***4.11 MODEL QUESTIONS***

1. What are ethics?
2. What is the moral importance of Computer Security?
3. How does computer security pose ethical issues?
4. What are safety-critical systems?
5. How compromises of confidentiality may violate privacy rights?
6. What are the moral responsibilities of Information Security professionals?
7. What are the ethical issues in computer security?
8. What is hacking? How it is different from cracking?
9. What are the two kinds of privacy issues raised by the Internet?
10. What is Ubiquitous Computing?
11. Define Ambient Intelligence.
12. What are the different tactics to ensure computer security and maintain privacy?

*REFERENCES, ARTICLE SOURCES AND CONTRIBUTORS*

- [1].(n.d.). Retrieved Jan. 27, 2016, from <https://en.wikipedia.org/wiki/E-governance> available under creative commons license.
- [2].(n.d.). Retrieved Nov. 04, 2015, from <http://www.pcg-services.com/resources/policies-procedures-barrier-growing-company/>
- [3].(n.d.). Retrieved Jan. 24, 2016, from <https://www.sans.org/reading-room/whitepapers/incident/protecting-insider-attacks-33168>
- [4].(n.d.). Retrieved Jan. 24, 2016, from <http://cert-in.org.in/>
- [5].(n.d.). Retrieved Jan. 25, 2016, from <https://www.sans.org/reading-room/whitepapers/detection/understanding-intrusion-detection-systems-337>
- [6].(n.d.). Retrieved Jan. 25, 2016, from <https://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901>
- [7].(n.d.). Retrieved an. 24, 2016, from <http://www.webopedia.com/>
- [8].(n.d.). Retrieved Jan. 25, 2016, from [https://en.wikipedia.org/wiki/Firewall\\_\(computing\)](https://en.wikipedia.org/wiki/Firewall_(computing))
- [9].(n.d.). Retrieved Jan. 25, 2016, from <http://social.technet.microsoft.com/wiki/contents/articles/10576.hardware-security-module-hsm.aspx>
- [10]. (n.d.). Retrieved Jan. 25, 2016, from [https://en.wikipedia.org/wiki/IT\\_asset\\_management](https://en.wikipedia.org/wiki/IT_asset_management)
- [11]. (n.d.). Retrieved from [https://en.wikipedia.org/wiki/Asset\\_\(computer\\_security\)](https://en.wikipedia.org/wiki/Asset_(computer_security))
- [12]. (n.d.). Retrieved Jan. 25, 2016, from <http://www.networkuptime.com/>
- [13]. (n.d.). Retrieved Jan. 25, 2016, from <http://techterms.com/>
- [14]. (n.d.). Retrieved Jan. 25, 2016, from <http://www.thewindowsclub.com/hardware-software-firewall-difference>
- [15]. (n.d.). Retrieved Jan. 25, 2016, from <http://www.itl.nist.gov/lab/bulletns/bltnmar03.htm>
- [16]. (n.d.). Retrieved Jan. 25, 2016, from [http://www.sersc.org/journals/IJMUE/vol3\\_no3\\_2008/8.pdf](http://www.sersc.org/journals/IJMUE/vol3_no3_2008/8.pdf)
- [17]. (n.d.). Retrieved Jan. 25, 2016, from <http://www.itl.nist.gov/lab/bulletns/bltnmar03.htm>
- [18]. (n.d.). Retrieved Jan. 25, 2016, from <https://www.sans.org/reading-room/whitepapers/vpns/overview-hardware-security-modules-757>
- [19]. (n.d.). Retrieved Jan. 25, 2016, from <https://www.pcisecuritystandards.org/documents/PCI%20HSM%20Security%20Requirements%20v1.0%20final.pdf>
- [20]. (n.d.). Retrieved Jan. 25, 2016, from [http://www.albany.edu/acc/courses/ia/acc661/NIST\\_SP\\_800-48.pdf](http://www.albany.edu/acc/courses/ia/acc661/NIST_SP_800-48.pdf)
- [21]. (n.d.). Retrieved Jan. 25, 2016, from [http://www.sersc.org/journals/IJMUE/vol3\\_no3\\_2008/8.pdf](http://www.sersc.org/journals/IJMUE/vol3_no3_2008/8.pdf)

- [22]. (n.d.). Retrieved Jan. 25, 2016, from <http://www.ironmountain.com/Knowledge-Center/Reference-Library/View-by-Document-Type/General-Articles/S/Secure-IT-Asset-Disposition-Your-Five-Step-Plan.aspx>
- [23]. (n.d.). Retrieved Jan. 25, 2016, from <http://searchmobilecomputing.techtarget.com/definition/Wi-Fi-Protected-Access>
- [24]. (n.d.). Retrieved Jan. 25, 2016, from [https://en.wikipedia.org/wiki/Wi-Fi\\_Protected\\_Access](https://en.wikipedia.org/wiki/Wi-Fi_Protected_Access)
- [25]. (n.d.). Retrieved from <http://techterms.com/>
- [26]. (n.d.). Retrieved from <http://www.cisco.com/>
- [27]. (n.d.). Retrieved Nov. 01, 2015, from <https://www.sbs.ox.ac.uk/cybersecurity-capacity/explore/home>
- [28]. (n.d.). Retrieved Jan. 03, 2016, from <http://live.sysinternals.com/tools/>
- [29]. (n.d.). Retrieved Jan. 03, 2016, from <http://www.moonsols.com/wp-content/plugins/download-monitor/download.php?id=7>
- [30]. (n.d.). Retrieved from <http://www.interpol.int/Crime-areas/Cybercrime/Cybercrime>
- [31]. (n.d.). Retrieved from <https://apwg.org/>
- [32]. (n.d.). Retrieved from <https://www.phishtank.com/>
- [33]. (n.d.). Retrieved from <http://www.ibtimes.co.uk>
- [34]. (n.d.). Retrieved Nov. 15, 2015, from [www.wikipedia.org](http://www.wikipedia.org)
- [35]. (n.d.). Retrieved Nov. 15, 2015, from [http://www.sentrillion.com/images/img\\_defense-in-depth.jpg](http://www.sentrillion.com/images/img_defense-in-depth.jpg)
- [36]. (n.d.). Retrieved Nov. 15, 2015, from [www.wikimedia.org](http://www.wikimedia.org)
- [37]. *An introduction to information security*. (n.d.). Retrieved FEB. 02, 2016, from <http://www.open.edu/openlearn/science-maths-technology/computing-and-ict/introduction-information-security/content-section-1> available under Creative Commons Attribution-NonCommercial-ShareAlike 4.0 Licence
- [38]. *Intrusion detection systems buyer's guide*. (n.d.). Retrieved Jan. 25, 2016, from <https://www.ipa.go.jp/security/fy11/report/contents/intrusion/ids-meeting/idsbg.pdf>
- [39]. The Wetware Group. (2012, march 22). *Hacking Wetware*. Retrieved Jan. 01, 2016, from <http://thewetwaregroup.blogspot.ca/p/other-methods.html>
- [40]. (2015, Oct. 30). Retrieved Nov. 01, 2015, from Department of Electronics and Information Technology: <http://deity.gov.in>
- [41]. 27000:2009, I. I. (2009). *Information technology - Security techniques - Information security management systems - Overview and vocabulary*. ISO/IEC.
- [42]. *Advanced Offensive Computer Security Training*. (n.d.). Retrieved Nov. 01, 2015, from <https://hakin9.org/>
- [43]. Alberts, C. a. (2003). *Managing Information Security Risks: The OCTAVE Approach*, . Addison-Wesley.

- [44]. Anderson, J. M. (2003). Why we need a new definition of information security. *Computers & Security*, , 308-313.
- [45]. Andress, J. (2011). *Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice*. Syngress.
- [46]. *Antivirus Software*. (2016). Retrieved Jan. 09, 2016, from Wikipedia: [https://en.wikipedia.org/wiki/Signature\\_based\\_detection#History](https://en.wikipedia.org/wiki/Signature_based_detection#History) available under creative commons sharealike license
- [47]. *Attack (computing)*. (n.d.). Retrieved Jan. 24, 2016, from [https://en.wikipedia.org/wiki/Attack\\_\(computing\)](https://en.wikipedia.org/wiki/Attack_(computing)) available under the Creative Commons Attribution-ShareAlike License.
- [48]. *BackTrack Linux – Penetration Testing Distribution*. (n.d.). Retrieved Nov. 01, 2015, from <http://www.backtrack-linux.org/>
- [49]. Banday, M. T. (2011). Emerging Challenges of Cyber Crimes to Cyber Security. Himanchal Pradesh: International Conference on Recent Advances in Electronics and Computer Engineering.
- [50]. Bhatt, K. (n.d.). *Information and Technology Act: Salient Features and Provisions*. Retrieved March 06, 2016, from <http://mrunal.org/2012/07/yearbook-it-act.html> available under the Creative Commons Attribution-Non Commercial-ShareAlike 4.0 License.
- [51]. Bunting, S., & Wei, W. (2006). *The Official EnCE: EnCase Certified Examiner Study Guide*. Wiley Publishing Inc.
- [52]. Caglar, S., & Savaser, S. (2010). Internet and child pornography. *International Journal of Human Sciences* , available under creative commons license.
- [53]. *Case Studies on Cyber Crimes*. (n.d.). Retrieved jan. 12, 2016, from <http://rtinagpur.cag.gov.in/uploads/CaseStudies/CaseStudiesonCyberCrimesNOTSENT/CaseStudiesonCyberCrimes.pdf>
- [54]. *CERT*. (2013, march 08). Retrieved Nov. 02, 2015, from [www.cert.org](http://www.cert.org)
- [55]. Commission, A. C. (2014). *Cybercrime*. Retrieved Mar. 01, 2016, from available under Creative Commons Attribution 3.0 Australia license
- [56]. (2010). *Committee on National Security Systems: National Information Assurance (IA) Glossary, CNSS Instruction No. 4009*.
- [57]. *Computer forensics*. (n.d.). Retrieved Jan. 09, 2016, from [https://en.wikipedia.org/wiki/Computer\\_forensics#Overview](https://en.wikipedia.org/wiki/Computer_forensics#Overview) available under the Creative Commons Attribution-ShareAlike License
- [58]. *Computer security incident management*. (n.d.). Retrieved Feb. 02, 2016, from Wikipedia: [https://en.wikipedia.org/wiki/Computer\\_security\\_incident\\_management](https://en.wikipedia.org/wiki/Computer_security_incident_management) available under creative commons sharealike license.
- [59]. *CYBER SECURITY MANIFESTO 2.0*. (2012, Oct. 01). Retrieved Sep. 26, 2015, from cybersecuritymanifesto: <http://cybersecuritymanifesto.com/>

- [60]. *CYBER SECURITY MANIFESTO 2.0*. (2012, Oct. 01). Retrieved Sep. 28, 2015, from cybersecuritymanifesto.com: <http://cybersecuritymanifesto.com/>
- [61]. *Cybercrime countermeasures*. (n.d.). Retrieved Jan. 24, 2016, from [https://en.wikipedia.org/wiki/Cybercrime\\_countermeasures](https://en.wikipedia.org/wiki/Cybercrime_countermeasures) available under the Creative Commons Attribution-ShareAlike License.
- [62]. *Cyberterrorism*. (n.d.). Retrieved March 06, 2016, from Wikipedia: <https://en.wikipedia.org/wiki/Cyberterrorism>
- [63]. Das, R. (2014, may 26). *Social Engineering Attacks*. Retrieved Jan. 01, 2016, from InfoSecBuss: <http://www.infosecbuzz.com/social-engineering-attacks/>
- [64]. *Department Of Electronics & Information Technology*. (n.d.). Retrieved Nov. 02, 2015, from <http://www.deity.gov.in/>
- [65]. *Department Of Electronics & Information Technology*. (n.d.). Retrieved Jan. 04, 2016, from <http://deity.gov.in/>
- [66]. Dhawan, N. (n.d.). *Information Technology Act - 2000*. Retrieved March 06, 2016, from Institute of Lifelong Learning, University of Delhi: <http://vle.du.ac.in/mod/book/view.php?id=9573&chapterid=15063> available under a Creative Commons Attribution-NonCommercial-ShareAlike 2.5 India License.
- [67]. Dhingra, A., & Misra, D. C. (2002). E-Governance Model. *Electronics Information & Planning (ISSN 0304-9876 Vol.29, No.6-7, Mar-Apr 2002)* .
- [68]. *Digital Signature*. (2016). Retrieved Jan. 09, 2016, from Wikipedia: [https://en.wikipedia.org/wiki/Digital\\_signature](https://en.wikipedia.org/wiki/Digital_signature) available under the Creative Commons Attribution-ShareAlike License
- [69]. Dolan, A. (2004, Feb. 10). *Social Engineering*. Retrieved Jan. 02, 2016, from SANS: <https://www.sans.org/reading-room/whitepapers/engineering/social-engineering-1365>
- [70]. *DSCI*. (n.d.). Retrieved Nov. 02, 2015, from <https://www.dsci.in>
- [71]. *E - Governance - Concept & Significance*. (2014). Retrieved Jan. 29, 2016, from <http://www.publicadministrationtheone.blogspot.in/2014/02/e-governance-concept-significance.html> available under creativecommons sharealike-noncommercial-noderivative license.
- [72]. *E-commerce*. (n.d.). Retrieved Jan. 30, 2016, from <https://ccit205.wikispaces.com/E-commerce#E-Commerce> Business Models available under a Creative Commons Attribution Share-Alike 2.5 License.
- [73]. *E-Commerce*. (n.d.). Retrieved Jan. 30, 2016, from <https://itgs.wikispaces.com/E-Commerce> available under a Creative Commons Attribution Share-Alike 2.5 License.
- [74]. *Electronic business*. (2016, Jan. 05). Retrieved Jan. 09, 2016, from Wikipedia: [https://en.wikipedia.org/wiki/Electronic\\_business](https://en.wikipedia.org/wiki/Electronic_business) available under the Creative Commons Attribution-ShareAlike License
- [75]. *European Union Agency for Network and Information Security*. (n.d.). Retrieved Jan. 04, 2016, from <https://www.enisa.europa.eu>

- [76]. *Federal Bureau of Investigation*. (n.d.). Retrieved from <https://www.fbi.gov/>
- [77]. Frank, B., & Odunayo, E. (n.d.). *APPROACH TO CYBER SECURITY ISSUES IN NIGERIA: CHALLENGES AND SOLUTION*. Retrieved Jan. 26, 2016, from <http://www.ijcrsee.com/index.php/ijcrsee/article/view/11/114> available under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License.
- [78]. Gallagher, S. (2013, Oct. 02). *We are not who we are*. Retrieved Sep. 26, 2015, from Security Blog: <https://securityblog.redhat.com/tag/two-factor-authentication/>
- [79]. Glass, E. (2003). *The NTLM Authentication Protocol and Security Support Provider*. Retrieved Sep. 26, 2015, from Sourceforge: <http://davenport.sourceforge.net/ntlm.html>
- [80]. González, G. (2014). *Internet and the world wide web are not the same thing – we explain why*. Retrieved Jan. 27, 2016, from <http://blogthinkbig.com/internet-and-the-world-wide-web/> available under creative commons Attribution-ShareAlike 3.0 Unported (CC BY-SA 3.0) license.
- [81]. (1998). How Email Works. In P. Grall, *How Internet Works* (p. 85). Que Corporation.
- [82]. Grant, R. M. (1998). *Contemporary Strategy Analysis (3rd edn)*, . Blackwell.
- [83]. Gupta, A. (2011, March 01). *Digital Forensic Analysis Using BackTrack, Part 1*. Retrieved Sep. 26, 2015, from opensourceforu: <http://opensourceforu.eyetimes.com/2011/03/digital-forensic-analysis-using-backtrack-part-1/>
- [84]. Hallsworth, M., & Rutter, J. (2011). *MAKING POLICY BETTER*. Institute for Government.
- [85]. Havercan, P. (2015, July 17). *A plain person's guide to Secure Sockets Layer*. Retrieved Sep. 26, 2015, from <http://peter.havercan.net/computing/plain-persons-guide-to-secure-sockets-layer.html>
- [86]. Hernandez, S. (2015). *he Official (ISC)2 Guide to the CCSP CBK*. Wiley.
- [87]. *How it works*. (2010, Jan. 17). Retrieved Sep. 26, 2015, from Wikidot: <http://pychatter.wikidot.com/how-it-works>
- [88]. *How to protect your computer data from outside threats*. (n.d.). Retrieved Jan. 24, 2016, from <http://www.combofix.org/how-to-protect-your-computer-data-from-outside-threats.php>
- [89]. *How to protect your information from physical threats*. (n.d.). Retrieved Jan. 10, 2016, from <https://info.securityinabox.org/default/book/export/html/138> available under a Creative Commons Attribution-Share Alike 3.0 Unported License.
- [90]. *How to Reveal a Fake Facebook Account*. (n.d.). Retrieved Sep. 27, 2015, from [www.wikihow.com: http://www.wikihow.com/Reveal-a-Fake-Facebook-Account](http://www.wikihow.com/Reveal-a-Fake-Facebook-Account)
- [91]. Howe, W. (2014, May 28). *A Brief History of Internet*. Retrieved Jan. 27, 2016, from <http://www.walthowe.com/navnet/history.html> available under a Creative Commons Attribution-Noncommercial-Share Alike 3.0 United States License.

- [92]. *ICANNwiki*. (2015). Retrieved Jan. 27, 2016, from Domain Name System: [http://icannwiki.com/Domain\\_Name\\_System](http://icannwiki.com/Domain_Name_System) available under Creative Commons Attribution-ShareAlike License.
- [93]. *Incident handling process*. (n.d.). Retrieved Jan. 25, 2016, from <https://www.enisa.europa.eu/activities/cert/support/incident-management/browsable/incident-handling-process>
- [94]. *Incident handling process*. (n.d.). Retrieved Jan. 25, 2016, from <https://www.enisa.europa.eu/activities/cert/support/incident-management/browsable/incident-handling-process>
- [95]. *Indian Computer Emergency Response Team*. (n.d.). Retrieved Nov. 01, 2015, from <http://cert-in.org.in>
- [96]. *Indian Computer Emergency Response Team*. (n.d.). Retrieved Nov. 02, 2015, from <http://cert-in.org.in/>
- [97]. *Indian Computer Emergency Response Team*. (n.d.). Retrieved Jan. 04, 2016, from <http://cert-in.org.in/>
- [98]. *Indian Cyber Emergency Response Team*. (n.d.). Retrieved Nov. 01, 2015, from <http://cert-in.org.in/>
- [99]. *Information security*. (n.d.). Retrieved Feb. 02, 2016, from Wikipedia: [https://en.wikipedia.org/wiki/Information\\_security](https://en.wikipedia.org/wiki/Information_security) available under creative commons sharealike license.
- [100]. *Information security*. (2015, Oct. 05). Retrieved Nov. 04, 2015, from [https://en.wikipedia.org/wiki/Security\\_policy](https://en.wikipedia.org/wiki/Security_policy)
- [101]. *Institute of Defense Studies and Analyses*. (n.d.). Retrieved Nov. 02, 2015, from <http://www.idsa.in>
- [102]. *International Standard Organization*. (n.d.). Retrieved Nov. 02, 2015, from <http://www.iso.org/>
- [103]. *Internet Applications and Services*. (n.d.). Retrieved Jan. 27, 2016, from [http://oer.nios.ac.in/wiki/oer/ictapplication/internetanditsusage/internet\\_applications\\_and\\_services.html](http://oer.nios.ac.in/wiki/oer/ictapplication/internetanditsusage/internet_applications_and_services.html) available under the Creative Commons Attribution Share Alike 3.0 License.
- [104]. *Internet security*. (n.d.). Retrieved Nov. 04, 2015, from [https://en.wikipedia.org/wiki/Internet\\_security](https://en.wikipedia.org/wiki/Internet_security)
- [105]. *Introduction to Digital Forensics*. (2011, Nov. 16). Retrieved Sep. 28, 2015, from Wikibooks: [https://en.wikibooks.org/wiki/Introduction\\_to\\_Digital\\_Forensics](https://en.wikibooks.org/wiki/Introduction_to_Digital_Forensics)
- [106]. *Intrusion Detection System*. (n.d.). Retrieved Jan. 25, 2016, from [https://en.wikipedia.org/wiki/Intrusion\\_detection\\_system](https://en.wikipedia.org/wiki/Intrusion_detection_system) available under creative commons sharealike license.
- [107]. *IP address*. (n.d.). Retrieved Jan. 27, 2016, from [https://en.wikipedia.org/wiki/IP\\_address](https://en.wikipedia.org/wiki/IP_address) available under Creative Commons Sharealike lincese.



- [108]. ISACA. (n.d.). Retrieved Nov. 02, 2015, from <https://www.isaca.org/Pages/default.aspx>
- [109]. ISACA. (2008). *Glossary of terms*. Retrieved Feb. 02, 2016, from <http://www.isaca.org/Knowledge-Center/Documents/Glossary/glossary.pdf>
- [110]. Itami, H. a. (1987). *Mobilizing Invisible Assets*, . Harvard University Press.
- [111]. ITGS. (n.d.). Retrieved March 06, 2016, from <https://itgs-417.wikispaces.com/17.-+Logic+Bombs+available+under+a+Creative+Commons+Attribution+Share-Alike+3.0+License>.
- [112]. ITU. (n.d.). Retrieved Jan. 04, 2016, from <http://www.itu.int/>
- [113]. Kent, K., Chevalier, S., Grance, T., & Dang, H. (2006). Retrieved Jan. 03, 2016, from NIST: <http://csrc.nist.gov/publications/nistpubs/800-86/SP800-86.pdf>
- [114]. *Kerberos Authentication*. (n.d.). Retrieved Sep. 26, 2015, from Interactiva: <http://computers.interactiva.org/Security/Authentication/Kerberos/>
- [115]. Keyur. (2011, Dec. 17). *How to destroy sensitive information*. Retrieved Jan. 10, 2016, from <http://tipsck.blogspot.in/2011/12/how-to-destroy-sensitive-information.html>
- [116]. Kruse, W. G., & Heiser, J. G. (2001). *Computer Forensics: Incident Response Essentials* . . Addison Wesley.
- [117]. Lewis, B. C. (n.d.). *Information Warfare*. Retrieved March 07, 2016, from <http://fas.org/irp/eprint/snyder/infowarfare.htm>
- [118]. Libicki, M. C. (1995, Aug.). *What is Information Warfare?* Retrieved march 06, 2016, from <http://handle.dtic.mil/100.2/ADA367662> courtesy Institute for National Strategic Studies, Washington, DC.
- [119]. McDermott, ., E., & Geer, D. (2001). Information security is information risk management. *Proceedings of the 2001 Workshop on New Security Paradigms NSPW '01* (pp. 97-104). ACM.
- [120]. Mehnle, J. (2010, April 17). *Sender Policy Framework*. Retrieved Sep. 28, 2015, from Openspf: <http://www.openspf.org/Introduction>
- [121]. *Ministry of Home Affairs*. (n.d.). Retrieved Nov. 02, 2015, from <http://www.mha.nic.in>
- [122]. Moses, R. (1992). Risk analysis and management Chapter 21 in Jackson, K M and Hruska, J, *Computer Security Reference Book*. Butterworth-Heinemann.
- [123]. Nath, V. (n.d.). *Digital Governance Initiative: Strategic application of knowledge and technologies for good governance*. Retrieved Jan. 29, 2016, from <http://www.digitalgovernance.org/index.php/models> adopted with permission.
- [124]. *National Crime record Bureau*. (n.d.). Retrieved Dec. 10, 2015, from <http://www.ncrb.gov.in/>
- [125]. *National Crime Records Bureau*. (n.d.). Retrieved Nov. 02, 2015, from <http://ncrb.gov.in>


- [126]. *National Cyber Security Policy-2013*. (2013, July 02). Retrieved Nov. 01, 2015, from Department Of Electronics & Information Technology, Government Of India: <http://deity.gov.in/content/national-cyber-security-policy-2013-1>
- [127]. *National Institute of Standards and Technology*. (2015, oct. 30). Retrieved Nov. 02, 2015, from <http://www.nist.gov/>
- [128]. Nelson, B., Phillips, A., & Steuart, C. (2009). *Guide to Computer Forensics and Investigations*. Cengage Learning.
- [129]. Nolan, R., O'Sullivan, C., Branson, J., & Waits, C. (2005). *First Responders guide to Computer Forensic*. CERT Training and Education.
- [130]. *Organised crime groups*. (n.d.). Retrieved Mar. 01, 2016, from <http://www.nationalcrimeagency.gov.uk/crime-threats/organised-crime-groups> available under open government license.
- [131]. *Organised Cybercrime*. (2013, July 30). Retrieved Mar. 01, 2016, from INDUSTRY OF ANONYMITY: <https://industryofanonymity.com/category/organised-crime-and-cybercrime/>
- [132]. Pande, J. (2016). *Introduction to Cyber Security*. Uttarakhand Open University available under creative common license.
- [133]. Parker, D. B. (1981). *Computer Security Management*,. Reston.
- [134]. *Password Authentication Protocol*. (2015, July 17). Retrieved Sep. 26, 2015, from WIKIPEDIA: [https://en.wikipedia.org/wiki/Password\\_Authentication\\_Protocol](https://en.wikipedia.org/wiki/Password_Authentication_Protocol)
- [135]. *Physical security*. (n.d.). Retrieved Nov. 04, 2015, from [https://en.wikipedia.org/wiki/Physical\\_security](https://en.wikipedia.org/wiki/Physical_security)
- [136]. Piplin, D. (2000). *Information security: Protecting the global enterprise*. New York: Hewlett-Packard Company.
- [137]. PJ. (n.d.). *What are Policies, Standards, Guidelines and Procedures?* Retrieved Nov. 04, 03, from <http://mindfulsecurity.com/2009/02/03/policies-standards-and-guidelines/>
- [138]. *Press Information Bureau* . (n.d.). Retrieved Nov. 02, 2015, from <http://pib.nic.in/>
- [139]. (2008). *PROMOTING e-GOVERNANCE : The SMART Way Forward*. Govt. of India.
- [140]. Quirk, S. (2014, Mar. 13). *Concordia Password Security Policy*. Retrieved Sep. 26, 2015, from <http://kb.cu-portland.edu/Password+Security>
- [141]. *Recognise scam or hoax emails and websites*. (n.d.). Retrieved Sep. 27, 2015, from <https://www.communications.gov.au>: <https://www.communications.gov.au/what-we-do/internet/stay-smart-online/your-identity/recognise-scam-or-hoax-emails-and-websites>
- [142]. Satheesh. (2009, Jaune 29). *Selected Case Studies on Cyber Crime*. Retrieved Jan. 12, 2016, from [http://satheeshgnair.blogspot.in/2009/06/selected-case-studies-on-cyber-crime.html#Insulting\\_Images\\_of\\_Warrior\\_Sh](http://satheeshgnair.blogspot.in/2009/06/selected-case-studies-on-cyber-crime.html#Insulting_Images_of_Warrior_Sh) available


- [143]. *Scam Watch*. (n.d.). Retrieved Jan. 12, 2016, from <https://www.scamwatch.gov.au> available under a Creative Commons Attribution 3.0 Australia
- [144]. Schmitz, A. (2012, Dec. 12). *Internet 101: Understanding How the Internet Works*. Retrieved Jan. 27, 2016, from <http://2012books.lardbucket.org/books/getting-the-most-out-of-information-systems-v1.3/s16-02-internet-101-understanding-how.html> available under Creative Commons by-nc-sa 3.0 license.
- [145]. *Secure Electronic Transaction*. (n.d.). Retrieved Jan. 09, 2016, from Wikipedia: [https://en.wikipedia.org/wiki/Secure\\_Electronic\\_Transaction#History\\_and\\_development](https://en.wikipedia.org/wiki/Secure_Electronic_Transaction#History_and_development) available under the Creative Commons Attribution-ShareAlike License
- [146]. *Security Threats*. (n.d.). Retrieved Jan. 24, 2016, from <https://msdn.microsoft.com/en-us/library/cc723507.aspx>
- [147]. *Selecting a strong password*. (2015, Sep. 10). Retrieved Sep. 26, 2015, from Wordpress: <https://en.support.wordpress.com/selecting-a-strong-password/>
- [148]. Shinde, D. (2005). *Ethical issues for IT security professionals*. Retrieved Feb. 02, 2016, from <http://www.computerworld.com/article/2557944/security0/ethical-issues-for-it-security-professionals.html> adopted for educational purpose.
- [149]. Singh, H., & Singh, G. (2013). Retrieved Jan. 25, 2016, from Wireless Networking Security: [http://www.ijarcse.com/docs/papers/Volume\\_3/5\\_May2013/V3I5-0178.pdf](http://www.ijarcse.com/docs/papers/Volume_3/5_May2013/V3I5-0178.pdf)
- [150]. STAGES OF e-GOVERNANCE. (2008). *WORKSHOP ON e-GOVERNANCE*. National Productivity Council with permission to reuse.
- [151]. Stewart, W. (2000, Jan. 07). *How Email Works*. Retrieved Sep. 28, 2015, from <http://www.livinginternet.com/>: <http://www.livinginternet.com/e/ew.htm>
- [152]. *Surveillance*. (n.d.). Retrieved March 06, 2016, from <https://en.wikipedia.org/wiki/Surveillance>
- [153]. *The Browser Exploitation Framework*. (n.d.). Retrieved Nov. 01, 2015, from <http://beefproject.com/>
- [154]. *The Information Warfare Site*. (2003, April 11). Retrieved March 06, 2016, from <http://www.iwar.org.uk/iwar/resources/wikipedia/information-warfare.htm> available under the terms of the GNU Free Documentation License.
- [155]. *The Open Group*. (n.d.). Retrieved Nov. 02, 2015, from [www.opengroup.org](http://www.opengroup.org)
- [156]. *The Open Web Application Security Project*. (2015, Sep. 30). Retrieved Nov. 01, 2015, from <https://www.owasp.org/>
- [157]. Tiwari, S. K. (2014). CYBER CRIMES: A THREAT TO HUMANITY. *Humanities & Social Sciences Reviews*, 94-101.
- [158]. Truong, Q. (2013, April 11). *The Cost of Cash*. Retrieved Jan. 31, 2016, from <http://sites.tufts.edu/costofcash/2013/04/11/google-wallet/> available under a Creative Commons Attribution-ShareAlike 3.0 United States License.
- [159]. Turer, P. (2007). Applying a Forensic Approach to Incident Response, Network Investigation and System Administration using Digital Evidence Bags. Digital

- Investigation . *he International Journal of Digital Forensics & Incident Response* , 30-35.
- [160]. Turnbull, N. (2003). 'Foreword' in Calder, Alan and Watkins, Steve, *IT Governance: A Manager's Guide to Data Security & BS 7799/ISO 17799 (2nd edn)*, Kogan Page (Set Book).
- [161]. *Understanding Authentication*. (2008, Feb. 14). Retrieved Sep. 26, 2015, from Go4Experts: <http://www.go4expert.com/articles/understanding-authentication-t8842/>
- [162]. *Vandalism*. (n.d.). Retrieved March 06, 2016, from <https://en.wikipedia.org/wiki/Vandalism>
- [163]. Venter, H. S., & Eloff, J. P. (2003). A taxonomy for information security technologies. *Computers & Security* , 299-307.
- [164]. Verma, D. (2012, Nov. 05). *How To Identify Fake EMail And Trace Sender's Location*. Retrieved Sep. 27, 2015, from <http://www.usethistip.com>: <http://www.usethistip.com/2012/11/how-to-identify-fake-email-and-trace.html>
- [165]. *Volatility Labs*. (2015, Nov. 30). Retrieved Jan. 03, 2016, from [www.volatility-labs.blogspot.com](http://www.volatility-labs.blogspot.com)
- [166]. Watson, R. T., Berthon, P., & Pitt, L. F. (n.d.). *Electronic Commerce Technology*. Retrieved Jan. 31, 2016, from <http://opentextbc.ca/electroniccommerce/chapter/electronic-commerce-technology/> available under a Creative Commons Attribution 4.0 International License.
- [167]. *Web Application Security Consortium* . (n.d.). Retrieved Nov. 01, 2015, from <http://www.webappsec.org>
- [168]. *What is a Firewall?* (n.d.). Retrieved Jan. 24, 2016, from <http://www.networkuptime.com/winfw/page01-01.html> available under creative commons license.
- [169]. *What is Outsider Attacks*. (n.d.). Retrieved Jan. 24, 2016, from <http://www.igi-global.com/dictionary/outsider-attacks/21648>
- [170]. *What Is the Difference between Hardware and Software Firewalls?* (2014). Retrieved Jan. 25, 2016, from <http://www.zonealarm.com/firewall-blog/blog/difference-hardware-software-firewalls/>
- [171]. Windley, P. (2002). Retrieved from <http://www.windley.com/docs/eGovernment%20Matu>
- [172]. Windley, P. J. (2002). *eGovernment Maturity*. Retrieved Jan. 30, 2016, from <http://www.windley.com/docs/eGovernment%20Maturity.pdf> (c)Copyright 2002, Phillip J. Windley with permission for reproduction for educational and research purpose
- [173]. *World Wide Web Jobs*. (n.d.). Retrieved Jan. 27, 2016, from <http://jobs.code4lib.org/jobs/world-wide-web/> available under creative commons license.
- [174]. York, D. (2014). *What Is A TLD? gTLD? ccTLD? newgTLD? IDN?* Retrieved Jan. 27, 2016, from <http://www.disruptiveconversations.com/2014/03/what-is-a-tld-gtld->

cctld-newgtld-idn.html available under a Creative Commons Attribution-NonCommercial-sharealike license.

[175]. Zeltser, L. (2010). *Incidence Response Plan*. Retrieved Jan. 25, 2016, from <http://security.uconn.edu/wp-content/uploads/sites/251/2014/05/security-incident-response-procedures.pdf>


Er. Saurav Joshi
Assistant Professor, Dept. Of ECE, Birla Institute of Applied Sciences, Bhimtal(Uttarakhand)
Email: saurav.rkt@gmail.com


Ms. Priyanka Tewari
IT Consultant, Chandigarh
Email: pinkytewari2008@gmail.com


Er. Ashutosh Bahuguna
Scientist at Indian Computer Emergency Response Team (CERT-In)
Email: bahuguna.a@deity.gov.in