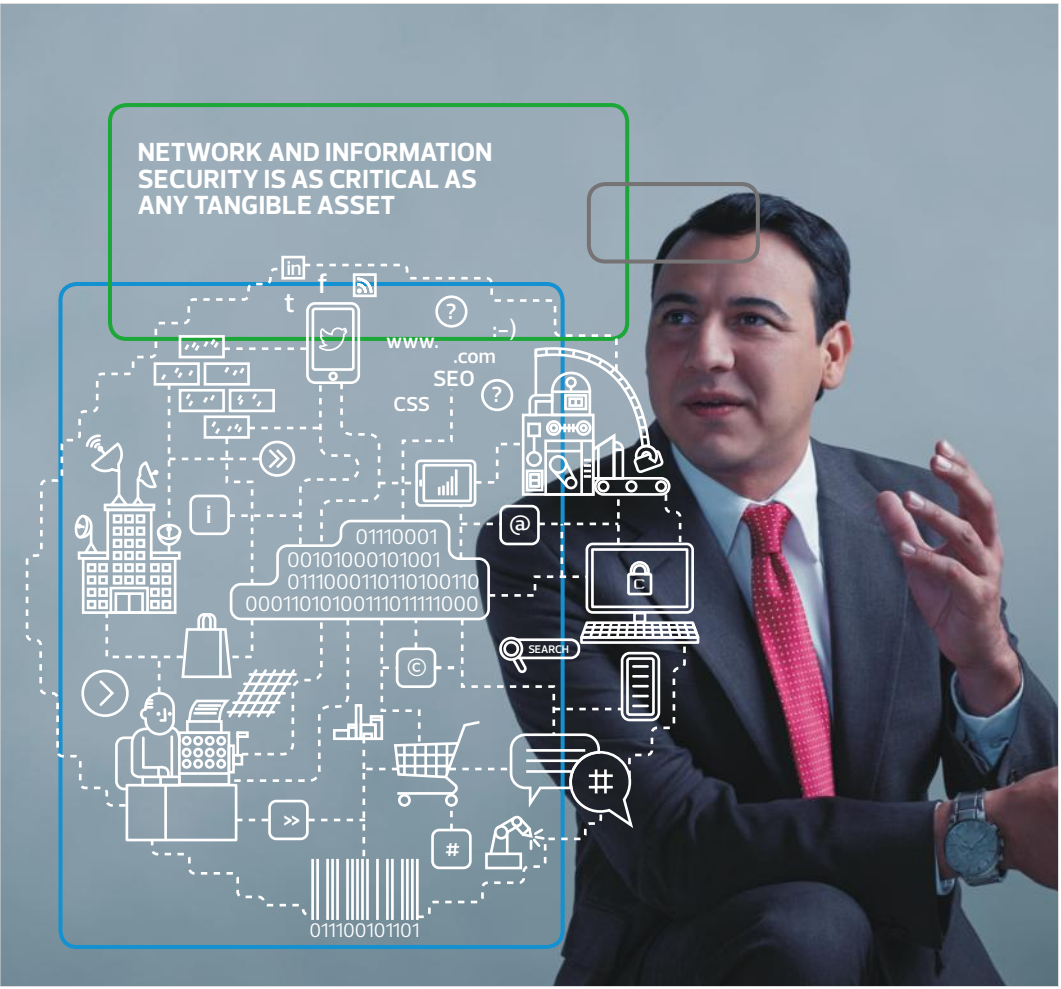


NETWORK SECURITY IN THE DIGITAL AGE

THE POWER OF BEING UNDERSTOOD

RSM

RSM in India

- Consistently ranked amongst India's top six accounting and consulting groups (International Accounting Bulletin, September 2015)
- Nationwide presence through offices in 12 key cities across India
- Multi-disciplinary personnel strength of over 1,200
- Empaneled as an IT Security Auditing Organisation with Cert-IN (Ministry of Telecommunications and Information Technology, Government of India)

rsmindia.in

RSM

- Seventh largest global audit, tax and consulting network
- Firms in over 110 countries and in each of the top 40 major business centres throughout the world
- Combined staff of over 37,500 in over 730 offices across the Americas, Europe, MENA, Africa and Asia Pacific

rsm.global

NETWORK SECURITY IN THE DIGITAL AGE

PREFACE

Information Technology (IT) Significance in Business

Information Technology (IT) has become a backbone for every business. It has permeated through every business today. In this digitalised era, 'Communication' is another important aspect, which plays a huge role in managing business functions. Companies rely on IT and other networks for the purpose of data processing, fast communications and acquiring market intelligence. Thus, 'Information' and 'Communication' are two of the most important strategic issues for the success of every enterprise.

Majority of the businesses have invested heavily in IT. The purchase of IT or network equipment continues to be the largest category of industry spending for all types of capital equipment. Almost all IT applications are dependent on network for variety of basic business activities.

Need for Network Security

IT networks are 'sensitive assets' for any business. They store, carry, and process huge amount of 'confidential' and 'high value' data through the internet. The use of data using remote access, cloud and mobile devices has made network security critical for the businesses from business, financial, legal and reputational perspectives. A single breach of IT / network security can result in colossal loss for business. Thus, protecting the IT network is crucial for every business. Larger enterprises design and build software products that need to be protected against attacks, data piracy, etc. Many network security approaches have been developed in a disorganised way by various organisations which have failed to actually secure assets or information. With proper network security approach in place, organisations would experience many business benefits such as meeting mandatory regulatory compliance requirements, preventing business disruption, etc. which helps keep employees productive.

In a recent survey conducted by the Computer Security Institute (CSI), 70% of the organisations polled stated that their network security defences had been breached and that 60% of the incidents came from within the organisations themselves. While it is difficult to measure how many companies have had internet-related security problems and the financial losses due to those problems, it is clear that the problems do exist and are widespread.

Ultimately, network security helps protect business reputation by avoiding financial losses or information disclosure, which is one of its most critical assets.

The purpose of network security is essentially to prevent loss through misuse of data. There are a number of potential pitfalls that may arise if network security is not implemented properly. Some of these are:

- **Breaches of confidentiality:** Each business will identify the need to keep certain critical information private from competitor eyes.
- **Data destruction:** Data is a valuable commodity for individuals and enterprises alike. It is a testament to its importance when the proliferation of backup technology available today is considered. Destruction of data can severely cripple the victim concerned.
- **Data manipulation:** A system break-in may be easily detectable, as some hackers tend to leave tokens of their accomplishment. However, data manipulation is a more insidious threat. Manipulation of data values may go unnoticed for a long duration or may not seem to be a serious concern initially. However, the significance becomes immediately apparent when financial information is involved.

Following are few examples of biggest security breaches in 2014

Organisation	What data compromised?	How hackers got into network?	For how long was the network hacked?	How was security breach discovered?
Sony	Almost all employees' details and sensitive information lying on network servers	Unknown, still in progress to find cause	Unknown	Employee computers received messages threatening public distribution of stolen data and displays of skulls on their screens
Target	40 million credit and debit cards, 70 million phone numbers, mailing addresses and email addresses	Hacking the credentials of a legitimate business associate, an HVAC company, to get on Target's network, then installing malware on point-of– sale machines	About 2 weeks	Anti-malware software flagged the problem and department of justice informed the company as well
Home Depot	Almost 56 million credit cards put at risk, 53 million email addresses	Via a third-party vendor's credentials followed up by exploiting an unpatched Windows flaw	About 6 months	The stores executives were informed by bank and law-enforcement officials
C&K Systems	8,68,000 credit and debit card numbers	By infecting point of sales card-swipe machines after compromising the network of the operator of the machines	Almost 18 months	Federal officials and payment card investigators informed the company

Following are few examples of biggest security breaches in 2014

Organisation	What data compromised?	How hackers got into network?	For how long was the network hacked?	How was security breach discovered?
JP Morgan	Phone numbers and email addresses for 76 million households plus 7 million small businesses	Criminals compromised the computer of an employee with special privileges that was used both at work and at home.	3 months	Investigations (within India and out of India)

Table 1: Biggest security breaches in year 2014 (source: www.networkworld.com)

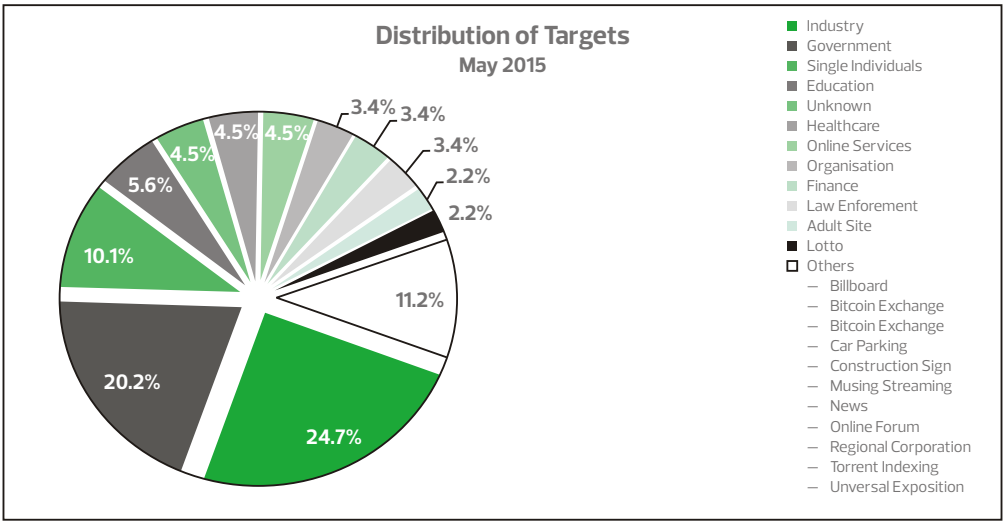
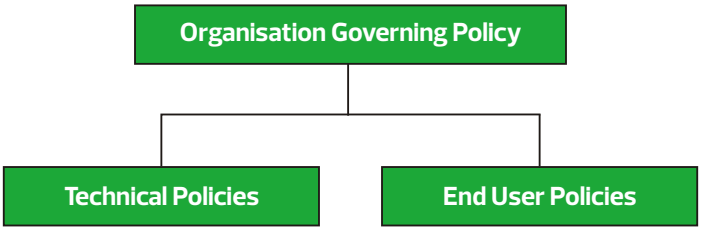


Figure 1 – Distribution of Attack Targets (Source: www.hackmageddon.com)

Defining Network Security Policy

In view of the above, it is imperative for any organisation to lay down a well-defined and comprehensive Network Security Policy to protect its information and data confidentiality and integrity objectives. A network security policy comprises of a set of objectives for the company, rules for users and administrators, and requirements for system and management that ensure the security of network and computer systems

in an organisation. A security policy is a 'living document', and needs to be continuously updated as technology and employee requirements change.



End-user policies are compiled into a single policy document that covers all the topics pertaining to information security that end users should know about, comply with, and implement. This policy may overlap with the technical policies and is at the same level as a technical policy. Grouping all the end-user policies together means that users have to go to only one place and read one document to learn everything that they need to do to ensure compliance with the company security policy.

Technical policies are also known as network security policies. Security staff members use the technical policies in the conduct of their daily security responsibilities. These policies are more detailed than the governing policy and are system or issue specific (e.g. router security issues or physical security issues). These policies are essentially security handbooks that describe what the security staff should do, but not how the security staff performs its functions.

The following are typical policy categories for technical policies.

- **General Policies**
  - **Risk-assessment policy:** Defines the requirements and provides the authority for the information security team to identify, assess, and remediate risks to the information infrastructure that is associated with conducting business.
  - **Data classification policy:** Defines the classification or categories of data based business context, nature of data, its criticality, sensitivity and usage and regulatory environment. Further, it will specify handling requirements for data based on their classification.

- **Acceptable use policy:** Defines the acceptable use of equipment and computing services, and the appropriate security measures that employees should take to protect the corporate resources and proprietary information.
- **Account access request policy:** Defines the account and access request process within the organisation. Users and system administrators who bypass the standard processes for account and access requests may cause legal action against the organisation.
- **Acquisition assessment policy:** Defines the responsibilities regarding corporate acquisitions and defines the minimum requirements that the information security group must complete for an acquisition assessment.
- **Audit policy:** Used to conduct audits and risk assessments to ensure integrity of information and resources, investigate incidents, ensure conformance to security policies, or monitor user and system activity where appropriate.
- **Information sensitivity policy:** Defines the requirements for classifying and securing information in a manner appropriate to its sensitivity level.
- **Password policy:** Defines the standards for creating, protecting, and changing strong passwords.
- **Global web server policy:** Defines the standards that are required by all web hosts.

■ **Email Policies**

- **Automatically forwarded email policy:** Defines the policy for restricting automatic email forwarding to any destination without prior approval from the appropriate manager or director.
- **Email policy:** Defines the standards to prevent ruination the public image of the organisation.

■ **Remote-access Policies**

- **Dial-in access policy:** Defines the appropriate dial-in access and its use by

authorised personnel.

- **Remote-access policy:** Defines the standards for connecting to the organisation network from any host or network outside the organisation.
- **VPN security policy:** Defines the requirements for remote-access IP Security (IPsec) or Layer 2 Tunnelling Protocol (L2TP) VPN connections to the organisation network.

- **Personal Device and Phone Policies:** Personal communication device policy defines the information security's requirements for personal communication devices, such as voicemail, smartphones, tablets, and so on.

- **Application Policies**
  - **Encryption policy:** Defines the requirements for encryption algorithms that are used within the organisation.
  - **Application service provider policy:** Defines the minimum security criteria that application service provider must execute before the organisation uses the service on a project.
  - **Database credentials coding policy:** Defines the requirements for securely storing and retrieving database usernames and passwords.
  - **Inter-process communications policy:** Defines the security requirements that any two or more processes must meet when they communicate with each other using a network socket or operating system socket.
  - **Project security policy:** Defines requirements for project managers to review all projects for possible security requirements.
  - **Source code protection policy:** Establishes minimum information security requirements for managing and storing product source code.

- **Network Policies**
  - **Extranet policy:** Defines the requirement that third-party organisations that need access to the organisation networks must sign a third-party

connection agreement.

- **Network access policy:** Defines the standards and minimum requirements for any device that requires connectivity to the internal network.
- **Network access standards:** Defines the standards for secure physical port access for all wired and wireless network data ports.
- **Network devices security policy:** Defines the security configuration standards for routers, switches and firewall inside a company production network or used in a production capacity.
- **Server security policy:** Defines the minimal security configuration standards for servers inside a company production network or used in a production capacity.

- **Wireless Security Policy:** Defines standards for wireless systems that are used to connect to the organisation networks.
- **Data Retention Policy:** Defines the systematic review, retention, and destruction of data or information received or created during the course of business. The categories of retention policy are, among others:
  - **Electronic communication retention policy:** Defines standards for the retention of email and instant messaging.
  - **Financial retention policy:** Defines standards for the retention of bank statements, annual reports, pay records, accounts payable and receivable, and so on.
  - **Employee records retention policy:** Defines standards for the retention of employee personal records.
  - **Operation records retention policy:** Defines standards for the retention of past inventories information, training manuals, suppliers lists, and so on.

Implementing Network Security

Network security can be achieved by implementing physical security of network resources and defining the proper access level for each system / user in network.

Physical network security is as important as or more important than logical (Software based) security—a failure in physical security can quickly abolish all the work done on the software side to secure network. However, this aspect of security is often overlooked or poorly planned. A solid network security plan should include a detailed review of physical security, including access control, surveillance, data center monitoring, and data backup.

IT departments of most of the businesses are largely adopting the Wi-Fi networks for better and easy access of network resources due to which an entirely new dimension of vulnerability and intruders is introduce to network security.

In this booklet, we have endeavoured to cover each of the above aspects at greater length. It must be emphasised that security in digital age is a dynamic subject.

Wish you a 'Secure' reading!

NETWORK SECURITY IN THE DIGITAL AGE

Table of Contents

1.0

INTRODUCTION TO NETWORK SECURITY

Chapter 1: Introduction to Network Security

1.1 What is Computer Network?

A computer network is a group of computer systems and other computing hardware devices that are linked together through communication channels to facilitate communication and resource-sharing among a wide range of users. The basic idea of networks is to allow people to access geographically distant resources without having to be physically present. It has also been designed to send data back and forth, to stay connected.

Computer networks are used to:

- Facilitate communication via email, video conferencing, instant messaging, etc.
- Enable multiple users to share a single hardware device like a printer or scanner
- Enable file sharing across the network
- Allow for the sharing of software or operating programs on remote systems
- Make information easier to access and maintain among network users

Types of Computer Networks:

- **Local Area Network (LAN):** A LAN is a type of computer network in which networking facilities are available in a small physical area probably in an office building, home, school or places like airport, hotel, etc. Each computer or device connected to network is called as node. LAN uses a transmission technology consisting of inexpensive hardware such as ethernet cables, to which all other devices and computers are attached.
- **Wide Area Network (WAN):** WAN is a computer network that covers a broad area, i.e. any network whose communication links cross metropolitan, regional or national boundaries. WAN can be thought of as a geographically dispersed collection of LANs which are connected to each other through a

network device called a router. Internet is the largest WAN covering the globe.

- **Metropolitan Area Network (MAN):** MAN is a computer network that covers area larger than LAN but smaller than WAN. The best example of a MAN is the cable television network available in many cities.

- **Personal Area Network (PAN):** PAN is a computer network used for communication among various computers and other communicating and information giving devices such as personal computers, printer, fax machines, telephones, PDAs, scanner etc. A PAN may include wired or wireless connection between devices.

- **Virtual Private Network (VPN):** VPN is a special type of secured network. VPN is used to provide a secure encrypted connection across a public network, such as an internet. Organisations typically use a VPN to provide a secure connection between a company and its known external users or offices. A VPN is generally less expensive to build and operate than a dedicated real network, because the virtual network shares the cost of system resources with other users of the real network.

- **Enterprise Private Network (EPN):** EPN is network built by an enterprise to interconnect various company sites such as production sites, head office, remote office and other sites to share network resources.

The diagram below depicts simple network architecture.

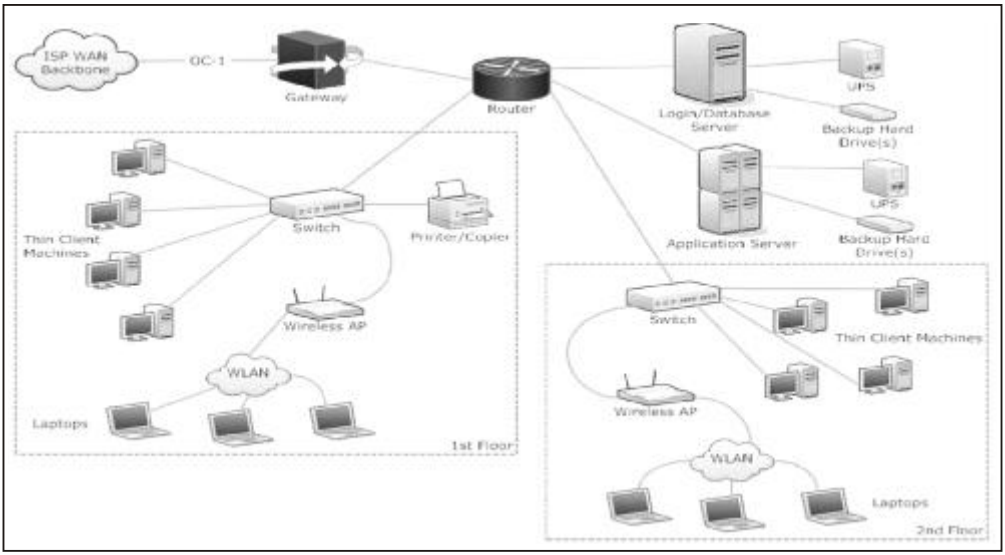


Figure 2 – Simple Network Architecture

1.2 What is Network Security?

Network security is the process of taking physical and software preventative measures to protect the underlying networking infrastructure from unauthorised access, misuse, malfunction, modification, destruction, improper disclosure and service disruption, thereby creating a secure platform for computers, users and programs to perform their permitted critical functions within a secure environment.

In simple words, network security is an organisation's strategy and provisions for ensuring the security of its assets and of all network traffic.

Network security is manifested in an implementation of security policy for hardware and software. Following are the key pillars of network security.

- **Security Policy:** The security policy is the principle document for network security. Its goal is to outline the rules for ensuring the security of organisational assets. Organisation today uses numerous tools/applications to conduct business productively. Policy that is driven by

the organisation's culture supports these routine and focuses on the safe enablement of these

tools or applications to its employees. The enforcement and auditing procedures for any regulatory compliance which an organisation is required to meet must be mapped out in the security policy.

- **Enforcement:** Enforcement of the network security policy means that the policy document is strictly adhered to maintain 'confidentiality', 'integrity' and 'availability' (CIA) of the organisation's assets.
  - **Confidentiality:** involves the protection of assets from unauthorised entities.
  - **Integrity:** ensuring the modification of assets is handled in a specified and authorised manner.
  - **Availability:** a state of the system in which authorised users have continuous access to said assets.

  Strong enforcement endeavours to provide CIA to the information flow in and out of network. This begins with the classification of information received or created by application, user and organisation. For the flow of any information via applications, all applications must first be identified by the firewall irrespective of other details like port, protocol, vague approach, or encryption. Proper identification of application provides basic visibility of the content it carries.

- **Auditing:** The auditing process of network security requires checking back the enforcement measures to determine how well they have aligned with the security policy. Auditing encourages continuous improvement by requiring the organisations to reflect the implementation of their policy on a consistent basis. This gives organisations an opportunity to adjust their policy and enforcement strategy in areas of evolving need.

1.3 Trends Affecting Network Security

Technology in the network security space has gone through many dramatic

changes recently. Evolvement of new trends such as use of different mobile operating systems, growing use of personal devices and Software-as-a-service (SaaS) delivery are challenging the network security. Network infrastructures are continuously getting enhanced to connect devices within or across the network. Following evolving trends may affect the network security practices of an organisation:

- **Mobile Networks, VPNs and Roaming Users:** Nowadays organisations require their employees to be connected to the network from anywhere from the globe. Maintaining connectivity to network from around the globe with enforced security is one of the biggest challenges for network security implementers. Network perimeter device like firewalls are gradually increasing features as most employees access network services from devices such as iPads, Android phones, tablets and PCs - need to be secured and in line to the security policy of organisation.

- **Targeted Attacks and APTs:** APTs (or advanced persistent threats) are basically next-generation network attacks in which unauthorised person gains network access and stays in the network undetected for long time. Normally APT attack is performed to steal data rather than to damage the data. Web filtering or IPS/IDS are used to identify and secure from such attacks which normally gets detected in first attempt or after initial compromise. Since attacker technology and new techniques are evolving rapidly, network security needs to be integrated with other security services to detect or prevent from such kind of attacks.

- **Bring Your Own Device (BYOD):** BYOD movement means user or customer can bring their own devices like iPads, iPhones and Android phones and connect to the corporate network. This kind of movement can be a challenge for network security implementers to secure the corporate data moving on user devices as network security endpoint agent may not have been deployed or may not be functioning properly on these devices. Organisation security strategy needs to create or enhance the BYOD policy to improve network security aspects.

- **Web Application and Web Server:** Web application attacks to extract data or malicious code distribution are very usual and will persist in future also.

Attackers compromise the legitimate web servers and use these servers to distribute their malicious code to other web servers. Any data-stealing attack which gets the attention of media can be a big threat for organisation as it may ruin the organisation's reputation in the market. Organisations need greater emphasis on protecting web servers and web applications as web server and web application technologies are evolving and similar challenges can be present for new technologies.

- **Cloud Services:** Enterprises with different business sizes are adopting the cloud services and Software as a Service (SaaS) for their business growth and connectivity. This trend creates a big challenge for network security, as network traffic can go beyond the traditional network checkpoints of inspection of data. Network security has to consider the scalability factor of the cloud and the information security consequences related to information lying on the cloud.

- **Encryption:** Organisations are deploying various kinds of data encryption at different layers to protect the privacy and integrity of data. However, more use of encryption will bring more challenges for network security devices to compute and understand the information.

- **Expanding Network:** Many organisations are focusing on extending connectivity to small branch or home offices. These changes to the size, scope and surface of network can lead to misconfiguration or change control errors that could lead to security breaches. Network security strategy needs to consider how to secure access across various platforms and small LANs over an expanding network perimeter.

2.0

DEFINING NETWORK SECURITY

Chapter 2: Defining Network Security

2.1 Know Your Network

Computer networks are designed to connect various systems like servers, clients/desktops, printers, etc. which operate on their local operating systems and are used to share the other network devices, software and data / information using different transmission media. In order to ensure good network security, implementer should know the network thoroughly and possible threats to it. Following information needs to be considered before implementing network security.

- **Types of servers in a network:** Servers are computers that hold shared files, programs, and the network operating system. Servers provide access to network resources to all the users of the network. There are various kinds of servers and one server can provide several functions. E.g. file servers, print servers, mail servers, communication servers, database servers, print servers, fax servers, web servers, etc.

- **Clients:** Clients are computers that access and use the network and shared network resources. Client computers are basically the customers (or users) of the network, as they request and receive services from the servers.

- **Type of transmission media being used:** Transmission media are the facilities used to interconnect computers in a network, such as twisted-pair wire, coaxial cable, and optical fibre cable. Transmission media are sometimes called channels, links or lines.

- **Which data are shared over network with clients?** Shared data are data that file servers or web servers provide to clients such as data files, web pages, printer access programs and e-mail.

- **How many shared printers and other peripherals are being used?** Shared printers and peripherals are hardware resources provided to the user of the network by servers. Resources provided include data files, printers, software, or any other items used by clients in the network

- **Which all network devices are in use and how are they functioning?** There can be multiple network devices being used at different layers of the network architecture. Generally, a network uses devices like firewall, router, switch, wireless router, IDS/IPS etc.

- **Which local operating systems are installed in servers and other devices?** A local operating system allows personal computers to access files, print to a local printer, and use one or more disk and CD drives that are located on the computer. Examples are MS-DOS, UNIX, Linux, windows 7, windows servers, etc.

- **Network Operating System :** The network operating system is a program that runs on computers and servers and allows the computers to communicate over the network.

2.2 Understand Network Security Threats and Attacks

2.2.1 Network Security Threats

Network security threat is any situation that poses harm to the computer network and can compromise the CIA of network or organisational data.

Fundamental threats related to network security are as follows:

- **Disclosure or Compromise:** Unauthorised disclosure of information

- **Deception:** Acceptance of false data

- **Disruption:** Interruption or prevention of correct data

- **Usurpation:** Unauthorised control of some part of system

2.2.2 Network Security Attacks

Network security attack can be any attempt to destroy, expose, alter, disable, steal or gain unauthorised access to or make unauthorised use of an asset or information. Common network / internet attack methods are broken down into categories. Some attacks are used to gain system knowledge or personal information and the other forms of attack are used to destroy or interrupt the

system functionality or availability.

There are multiple attacks which may attempt to make a threat reality; few are listed below.

- **Virus :** A computer virus is small software that can spread from one infected computer to another. The virus can corrupt, steal, or delete data on the computer and even erase anything from the hard drive. A virus can also spread itself to other computers through email programs.

- **Worms and Trojans:** A worm is similar to a virus because they both are self replicating, but th worm does not require a file to allow it to propagate. Trojans appear to be benign programs to the user, but actually have some malicious purpose. Trojans usually carry some payload such as a virus.

- **Data Sniffing:** Packet sniffing is the interception of data packets traversing a network. A sniffer program works at the ethernet layer in combination with network interface cards (NIC) to capture all traffic traveling to and from internet host site. Further, if any of the Ethernet NIC cards are in promiscuous mode, the sniffer program will pick up all communication packets floating–by anywhere near the internet host site. Most of packet sniffers are passive and they sniff (listen) all data link layer frames passing through the device's network interface. There are many of freely available packet sniffer programs on the internet. The more sophisticated ones allow more active intrusion.

- **Eavesdropping:** Eavesdropping is basically listening to the private conversation of other without their consent. Majority of network communications happens over insecure or unencrypted channels i.e. in clear–text format which allows an attacker who has already gained access to data paths in the network to 'listen' or interpret (read) the traffic. Process of eavesdropping on network communications is also referred as sniffing or snooping. Eavesdropping can also be done over telephone lines (wiretapping),email, instant messaging, an other methods of communication considered private.

- **Data Modification:** After an attacker has sniffed the data over network, the

next phase is to modify it. Data modification attack involves the alteration, insertion or deletion of data or information in unauthorised manner. An attacker can modify the data in the packet without the knowledge of the sender or receiver. These attacks are very difficult to detect. Website defacements are common examples of data modification attack.

- **Identity Spoofing (IP Address Spoofing):** Most networks and operating systems use the IP address of a computer to identify a valid entity. IP spoofing attack is to make the data appear as if it has come from a trusted host or IP when it really did not. An attacker might also use special constructed IP packets that appear to originate from valid addresses inside the corporate intranet network. After gaining access to the network with a valid IP address, the attacker can modify, reroute, or delete data.

- **Man-in-the-Middle Attack (Hijacking):** As the name indicates, a man-in-the-middle attack occurs when someone (attacker) between sender and the receiver who are communicating is actively monitoring, capturing, and controlling their communication transparently. E.g., the attacker can re-route a data exchange. When computers are communicating at low levels of the network layer, the computers might not be able to determine with whom they are exchanging data.

  Man-in-the-middle attacks are like someone pretends sender identity in order to read his message. The receiver on the other end might believe it is legitimate sender because the attacker might be actively replying as sender to keep the exchange going and gain more information.

- **Denial of Service (DoS):** Denial of Service is an attack when the system receiving too many requests cannot return communication with the requestors. The system then consumes resources waiting for the handshake to complete. Eventually, the system cannot respond to any more requests rendering it without service.

  A DoS attack can be perpetrated in a number of ways. There are three basic types of attack.

  — Consumption of computational resources, such as band width, disk

space or CPU time.

— Disruption of configuration information, such as routing information.

— Disruption of physical network components.

Common forms of DoS attacks are:

— **Buffer overflow attack:** The most common DoS attack is simply to send more traffic to a network address than the programmer's expectation on size of buffers. A few of the better known attacks based on the buffer characteristics of a program or system include:

- Sending e-mail messages that have attachments with 256 character file names to Netscape and Microsoft mail programs.
- Sending oversized Internet Control Message Protocol (ICMP) packets.
- Sending an e-mail message with a 'From' address longer than 256 characters.

— **Smurf attack:** In this attack, the perpetrator sends an IP ping request to a receiving site. The ping packet specifies that, it is broadcast to a number of hosts within the receiving site's local network. The packet also indicates that the request is from another site, which is the target site that is to receive the denial of service attack. The result will be lots of ping replies flooding back to the innocent, spoofed host. If the flood is great enough, the spoofed host will no longer be able to receive or distinguish real traffic.

— **SYN flood:** When a computer wants to make a TCP/IP connection to another computer, usually a server, an exchange of TCP/SYN and TCP/ACK packets of information occur. The computer requesting the connection, usually the client's or user's computer sends a TCP/SYN packet which asks the server if it can connect. If the server is ready, it responds a TCP/SYN-ACK packet back to the client to provide acknowledgement that it can connect and reserves a space

or session for the connection, waiting for the client to respond with a TCP/ACK packet. In a SYN flood, the address of the client is often forged so that when the server sends a TCP/SYN-ACK packet back to the client, the message is never received from client because the client either doesn't exist or wasn't expecting the packet and subsequently overlooks it. This leaves the server with a dead or open connection, reserved for a client that will never respond. Usually this is done to one server many times in order to reserve all the connections for unresolved clients, which prevents legitimate clients from making connections.

- **Distributed Denial-of-Service attacks (DDoS):** A distributed denial of service attack (DDoS) occurs when multiple compromised systems or multiple attackers flood the bandwidth or resources of a targeted system with useless or redundant traffic. These systems are compromised by attackers using a variety of methods.

  In DDoS attacks, the attacker first gains access to user accounts on numerous hosts across the internet. The attacker then installs and runs a slave program at each compromised site that quietly waits for commands from a master program running, the master program then contacts the slave programs, instructing each of them to launch a denial-of-service attack directed at the same target host. The resulting coordinated attack is particularly devastating, since it comes from so many attacking hosts at the same time.

- **Application-Layer Attack:** An application-layer attack targets application or web servers by deliberately causing a fault in a server's operating system or applications. This results in the attacker gaining the ability to bypass normal access controls. The attacker takes advantage of this situation, gaining control of application, system, or network, and can do any of the following:

  - Read, add, delete, or modify data or operating system.
  - Introduce a virus program that uses corporate computers and software applications to copy viruses throughout corporate network.

- Introduce a sniffer program to analyse network and gain information that can eventually be used to crash or to corrupt systems and network.
- Abnormally terminate data applications or operating systems.
- Disable other security controls to enable future attacks.

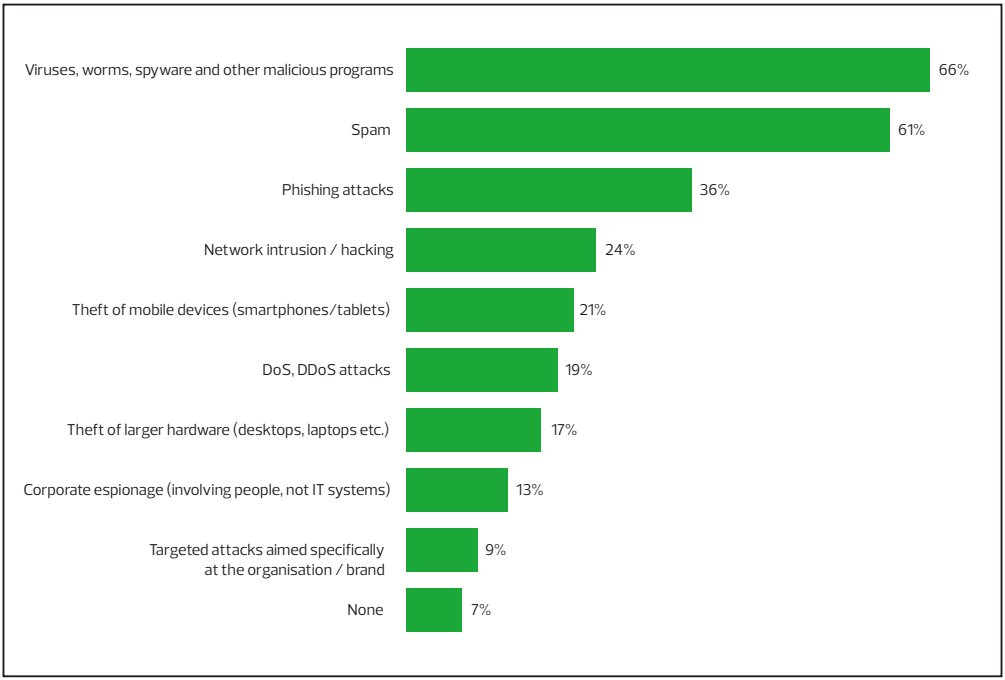
- **Social Engineering:** Social engineering is the use of influence or deception to gain access to information systems. The medium is usually a telephone or e-mail message. The attacker usually pretends to be a director or manager in the company traveling on business with a deadline to get some important data left on their network drive. They pressure the help desk to give them the toll-free number of the RAS server to dial and sometimes get their password reset. The main purpose behind social engineering is to place the human factor in the network-breaching loop and use it as a weapon. The human factor has been referred to as the weakest link in network security.

  Followings are few examples of social engineering attack:

  - **Fake Email:** The social engineer sends a message to one or more users in a domain that 'this is the system administrator and your password must be reset to user 123' for a temporary period of time. The hacker then continuously monitors the change and then exploits the whole system.
  - **Fictitious Competition:** The social engineer manipulates a group of users to participate in some fake competition for a jackpot prize, with the ultimate purpose of eventually extracting confidential information about network and password security.
  - **Phishing:** Phishing is an attempt to acquire sensitive information such as usernames, passwords, and credit card details (and sometimes, indirectly, money), often for malicious reasons, by impersonating as a trustworthy entity in an electronic communication.
  - **Pharming:** It is an attack intended to redirect a website's traffic to another, fake site. Pharming can be conducted either by changing the

hosts file on a victim's computer or by exploitation of a vulnerability in DNS server software. Compromised DNS servers are sometimes referred to as 'poisoned'. Pharming requires unprotected access to target a computer, such as altering a customer's home computer, rather than a corporate business server.

— **The helpful help desk:** The help desk gets a call from the social engineer impersonating a user reporting a forgotten password. In many cases the help desk will change the user's password over the phone. The hacker now has a legitimate user name and password to work with. To avoid problems from the original user, the social engineer will then call the user who was impersonated and say something like "This is Deepak from IT department. We had some problems with mail server today, so we are assuring mail service with users, can I have your password to check for the mail reception on your email id."



2.3 Define Network Security Policy

A security policy comprises of a set of objectives for the company, rules for users and administrators, and requirements for system and management that ensure the security of network and computer systems in an organisation. A security policy is a 'living document', and needs to be continuously updated as technology and employee requirements change.

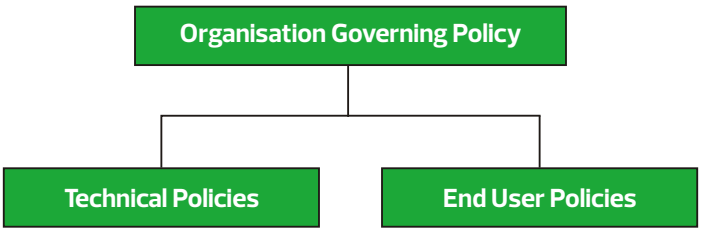
The security policy translates, clarifies, and communicates the management position on security as defined in high-level security principles. The security policy acts as a bridge between these management objectives and specific security requirements. It informs all level of users their obligatory requirements for protecting technology and information assets. It should specify the mechanisms that organisation need to meet these requirements. It also provides a baseline from which to acquire, configure, and audit computer systems and networks for compliance with the security policy. Therefore, an attempt to use a set of security tools in the absence of at least an implied security policy is meaningless.

Why Security Policy?

- To inform users, staff, and managers and make them accountable
- To specify mechanisms for security
- To provide a baseline

Security Policy Components

Below diagram shows the hierarchy of a corporate policy structure that is aimed at effectively meeting the needs of all audiences.



2.3.1 Organisation Governing Policy

The organisation's governing policy outlines the security concepts that are important to the company for all stakeholders and technical custodians:

- It controls all security-related interactions among business units and supporting departments in the company.
- It aligns closely with not only existing company policies, especially human resource policies, but also any other policy that mentions security-related issues, such as issues concerning email, computer use, or related IT subjects.
- It is placed at the same level as all companywide policies.
- It supports the technical and end-user policies.
- It includes the following key components:
  - A statement of the issue that the policy addresses
  - A statement about employee's position as IT manager on the policy
  - How the policy applies in the environment
  - The roles and responsibilities of those affected by the policy
  - What level of compliance to the policy is necessary
  - Which actions, activities, and processes are allowed and which are not
  - What the consequences of noncompliance are

2.3.2 End-User Policies

End-user policies are compiled into a single policy document that covers all the topics pertaining to information security that end users should know about, comply with, and implement. This policy may overlap with the technical policies and is at the same level as a technical policy. Grouping all the end-user policies

together means that users have to go to only one place and read one document to learn everything that they need to do to ensure compliance with the company security policy.

2.3.3 Technical Policies

Technical policies are also known as network security policies. Security staff members use the technical policies in the conduct of their daily security responsibilities. These policies are more detailed than the governing policy and are system or issue specific (for example, router security issues or physical security issues). These policies are essentially security handbooks that describe what the security staffs should do, but not how the security staffs performs its functions.

The following are typical policy categories for technical policies.

- **General Policies**
  - **Risk-assessment policy:** Defines the requirements and provides the authority for the information security team to identify, assess, and remediate risks to the information infrastructure that is associated with conducting business.
  - **Data classification policy:** Defines the classification or categories of data based business context, nature of data, its criticality, sensitivit and usage and regulatory environment. Further it will specify handlin requirements for data based on their classification.
  - **Acceptable use policy:** Defines the acceptable use of equipment and computing services, and the appropriate security measures that employees should take to protect the corporate resources and proprietary information.
  - **Account access request policy:** Defines the account and access request process within the organisation. Users and system administrators who bypass the standard processes for account and access requests may cause legal action against the organisation.
  - **Acquisition assessment policy:** Defines the responsibilities regarding

corporate acquisitions and defines the minimum requirements that the information security group must complete for an acquisition assessment.

- **Audit policy:** Used to conduct audits and risk assessments to ensure integrity of information and resources, investigate incidents, ensure conformance to security policies, or monitor user and system activity where appropriate.
- **Information sensitivity policy:** Defines the requirements for classifying and securing information in a manner appropriate to its sensitivity level.
- **Password policy:** Defines the standards for creating, protecting, and changing strong passwords.
- **Global web server policy:** Defines the standards that are required by all web hosts.

- **Email Policies**
  - **Automatically forwarded email policy:** Defines the policy for restricting automatic email forwarding to any destination without prior approval from the appropriate manager or director.
  - **Email policy:** Defines the standards to prevent ruination the public image of the organisation.
- **Remote-access Policies**
  - **Dial-in access policy:** Defines the appropriate dial-in access and its use by authorised personnel.
  - **Remote-access policy:** Defines the standards for connecting to the organisation network from any host or network outside the organisation.
  - **VPN security policy:** Defines the requirements for remote-access IP Security (IPsec) or Layer 2 Tunnelling Protocol (L2TP) VPN

connections to the organisation network.

- **Personal device and phone policies:** Personal communication device policy defines the information security's requirements for personal communication devices, such as voicemail, smartphones, tablets, and so on.

- **Application Policies**

  - **Encryption policy:** Defines the requirements for encryption algorithms that are used within the organisation.

  - **Application service provider policy:** Defines the minimum security criteria that application service provider must execute before the organisation uses the service on a project.

  - **Database credentials coding policy:** Defines the requirements for securely storing and retrieving database usernames and passwords.

  - **Inter-process communications policy:** Defines the security requirements that any two or more processes must meet when they communicate with each other using a network socket or operating system socket.

  - **Project security policy:** Defines requirements for project managers to review all projects for possible security requirements.

  - **Source code protection policy:** Establishes minimum information security requirements for managing and storing product source code.

- **Network Policies**

  - **Extranet policy:** Defines the requirement that third-party organisations that need access to the organisation networks must sign a third-party connection agreement.

  - **Network access policy:** Defines the standards and minimum requirements for any device that requires connectivity to the internal

network.

- **Network access standards:** Defines the standards for secure physical port access for all wired and wireless network data ports.
- **Network devices security policy:** Defines the security configuration standards for routers, switches and firewall inside a company production network or used in a production capacity.
- **Server security policy:** Defines the minimal security configuration standards for servers inside a company production network or used in a production capacity.

- **Wireless Security Policy:** Defines standards for wireless systems that are used to connect to the organisation networks.
- **Data Retention Policy:** Defines the systematic review, retention, and destruction of data or information received or created during the course of business. The categories of retention policy are, among others:
  - **Electronic communication retention policy:** Defines standards for the retention of email and instant messaging.
  - **Financial retention policy:** Defines standards for the retention of bank statements, annual reports, pay records, accounts payable and receivable, and so on.
  - **Employee records retention policy:** Defines standards for the retention of employee personal records.
  - **Operation records retention policy:** Defines standards for the retention of past inventories information, training manuals, suppliers lists, and so on.

3.0

IMPLEMENTING NETWORK SECURITY

Chapter 3: Implementing Network Security

Network security can be achieved by implementing physical security of network resources and defining the proper access level for each system / user in network.

3.1 Physical and Environmental Security

Unrestricted physical access to a computer or a network is the foremost security threat. If a hacker has physical access to network, stealing information is easy for him. The fastest way of accessing information over network is not through the firewall, but through a USB port on an unattended workstation/server. The most dangerous information thief may not be a distant hacker, but can be one of the cleaning staff inside corporate building. There is virtually no end to the ways people with spiteful intent can damage or steal data if they have simple physical access of network asset.

For instances, intruder can:

- Damage corporate equipment using the simple smashing or kicking asset.
- Use a tiny USB flash drive to steal data or insert a harmful virus.
- Steal or copy a hard drive and take it away to examine data.
- Install unauthorised software on unattended server or workstation.
- Boot a computer from a floppy disk and reformat the hard drive.
- Override password protection on a computer by opening the case and replacing the BIOS chip.
- Use a handheld device such as an iPod, cell phone, or digital camera to pull data out of system.

Physical network security is as important as or more important than logical (software based) security—a failure in physical security can quickly abolish all the work done on the software side to secure network. However, this aspect of security is often overlooked or poorly planned. A solid network security plan should include a detailed review of physical security, including access control,

surveillance, data center monitoring, and data backup. Following are basic elements which can be considered for physical and environmental security implementation:

- **Using Door Locks:** Every organisation has a server room which is used to keep servers, routers, switches, cables and other network devices. Anyone with physical access to server room can do enormous damage to network assets kept in that room. To prevent any type of physical damage of network assets, it is required to put good locks on server room door.

- **Using Electronic Access System:** Entire building of the organisation (i.e. where the servers and networks are placed) should be physical access controlled i.e. only authorised person should be allowed to enter in the required premise.

  Electronic access system using cards, tokens or biometrics should be used to provide access to locked doors or secured IT areas. An electronic access system tracks each user individually and creates a log showing who gained or requested access to the room. Additionally, these systems enable the organisation to customize access, so that each person can enter different areas within the facility.

  The most secure kind of door lock, by far, is the biometric access system. Biometrics is a technology that measures physiological characteristics, such as fingerprints, irises, voices, faces, and hands, for authentication purposes. Biometric authentication is becoming a popular way to identify people for security purposes since it has the advantage of being both more convenient and more secure than traditional card readers.

- **Using Security Surveillance Camera:** Keeping all network critical network assets in locked server room and providing access of that room to only authorised people using and electronic access system is initial steps to secure assets, but someone could break in, or someone who has authorised access could misuse that physical access. video surveillance camera placed in server room or premises which is difficult to tamper with or disable but gives good understanding of persons entering and leaving the server room or premises. Surveillance cameras can be set to monitor

continuously, or can use motion detection technology to record only when someone is moving about. They can even be set up to send e-mail or cell phone notification if motion is detected when it should not be (such as after hours). Finally, explicit notification of surveillance and strategically placed 'dummy' camera can discourage trouble by making people believe they're being watched.

- **Selecting Appropriate Transmission Medium and its Protection:** Transmission media is used to connect one network device to other network devices. While defining physical security aspect of network, it is very essential to consider the type of transmission media or network cable need to be used. The physical transmission medium for a wired network involves mainly twisted pair (copper) or Fiber optic cables. Selection of appropriate cable can be decided based on the network size and data transmission rates. Majorly LAN networks uses twisted pair cable to access the network devices. For larger network size with isolated small LAN connected and higher transmission rate is required, prefer use of Fiber cable over copper twisted pair cable to connect small LANs. Fiber optic cable doesn't radiate signals and is extremely difficult to tap.

- **Laptop Computer Lock:** Laptop computers are very commonly used in the organisations and store lot of sensitive corporate information. Laptop computers security deserves special consideration because their small size and portability makes them extremely vulnerable to loss and data theft. A stolen laptop can disclose sensitive information; also it can provide hacker a convenient way to enter into corporate network.

  Many laptop theft cases have been registered or observed in corporate premises. To protect laptop theft either use laptop with a docking station that can lock the laptop securely in place or lock laptop in a secure desk, cabinet or specially designed laptop lockbox. Also, laptop data should be encrypted to reduce the probability of sensitive information disclosure, if laptop is lost or stolen.

- **Secure In/Out Devices**

  — **USB port devices:** USB storage technology is emerging to allow

massive amount of data to be stored and transferred at higher speed. USB devices are getting smaller in size and bigger in storage as well as data transfer speed. Corporate employee with wrong (unusual) intentions can use this USB device to download sensitive data and upload potentially harmful apps or virus. USB ports are universal i.e. every desktop or laptop has minimum one USB port which is very easy to access and use. A small USB flash drive can easily hold 8 GB or more data which is sufficient to pull sensitive data from system without concern of administrator. Organisation should consider USB port block or restricted access on computers.

- **Banning handheld electronic devices:** Many of today's small electronic devices such as iPod MP3 players, cell phones, digital cameras, and PDAs contain a vast amount of memory and can be adapted to suck data out of a computer right through a USB port. If there is secure zone (severs having sensitive data) on network and organisation is extremely concerned about security breaches, banning these handheld devices in that zone is definitely something to consider in security plan.

- **Environmental Monitoring:** One of the foremost physical security measures is is to ensure that network devices are always kept in a safe, well-regulated environment. Environmental factors are of special concern when equipment is installed in remote, unsupervised locations.

  With proper environmental monitoring, it can be alerted to any conditions that can have a contrary effect on mission-critical equipment. Environmental monitoring products can also alert the potential damage from human error, hacking, or snooping fingers. Many systems can be combined with video monitoring so that it can keep an eye on network equipment as well as monitor conditions.

- **Surge and Power Protection:** Networking devices generally require a steady, uninterrupted power supply. Electricity is generally affordable, clean, and reliable, but it is subject to fluctuations. Too much voltage (surges and spikes) or too little voltage (power outages) can damage network equipment or make it temporarily unusable.

Organisation should use an Uninterrupted Power Supply (UPS) system to protect network equipment from damage due to power fluctuation. UPS system keeps the power flowing, giving enough time to shut down safely during a power outage.

- **Network Segregation:** Properly segregating the network can essentially minimizes the level of access to sensitive information for those applications, servers, and people who do not need it, while enabling access for those that do. Meanwhile segregation makes it much more difficult for a cyber-attacker to locate and gain access to organisation's most sensitive information

3.2 Logical Access Security

Logical security refers to the process of using hardware or software based techniques for authenticating a user's privileges on a specific computer network or system. The concept is a part of the more complete field of computer security, which involves both hardware and software methods for securing a terminal or network.

Logical security prevents unauthorised users from connecting or gaining access to system resources before and after achieving a physical connection to any one of network systems.

Following factors can be considered for logical access security implementation:

3.2.1 Identification and Authentication

Identification and Authentication is a critical building block of computer security since these are the basis for most types of access control and for establishing user accountability. Identification and Authentication is a technical measure that prevents unauthorised people (or unauthorised processes) from entering into an IT system. Access control usually requires that the system be able to identify and differentiate among users. For example, access control is often based on least privilege, which refers to the granting to users of only those accesses minimally required to perform their duties. User accountability requires the linking of activities on an IT system to specific individuals and, therefore, requires the system to identify users.

- **Identification:** Identification is the means by which a user provides a claimed identity to the system. The most common form of identification is the user ID.

  The following should be considered when using user IDs:

  - **Unique identification:** An organisation should require users to identify themselves uniquely before being allowed to perform any actions on the system unless user anonymity or other factors dictate otherwise.

  - **Correlate actions to users:** The system should internally maintain the identity of all active users and be able to link actions to specific users.

  - **Maintenance of user IDs:** An organisation should ensure that all user IDs belong to currently authorised users. Identification data must be kept current by adding new users and deleting former users.

  - **Inactive user IDs:** User IDs that are inactive on the system for a specific period of time (e.g., 3 months) should be disabled.

- **Authentication:** Authentication is the means of establishing the validity of user claim. There are three means of authenticating a user's identity which can be used alone or in combination, something, say, the individual knows (a secret -- e.g. a password, Personal Identification Number (PIN), or cryptographic key); something the individual possesses (E.g. an ATM card or a smart card or token); and something the individual is (a biometric, e.g. characteristics such as a voice pattern, retina, handwriting dynamics, or a fingerprint). The following aspects should be considered while implementing user authentication.

  - **Require the users to authenticate:** An organisation should require users to authenticate their claimed identities on IT systems. It may be desirable for users to authenticate themselves with a single log-in. This requires the user to authenticate them only once and then be able to access a wide variety of applications and data available on local and remote systems.

- **Restrict access to authentication data:** An organisation should restrict access to authentication data. Authentication data should be protected with access controls and one-way encryption to prevent unauthorised individuals, including system administrators, or hackers from obtaining the data.

- **Secure transmission of authentication data:** An organisation should protect authentication data transmitted over public or shared data networks. When authentication data, such as a password, is transmitted to an IT system, it can be electronically monitored. This can happen on the network used to transmit the password or on the IT system itself. Simple encryption of a password that will be used again does not solve this problem because encrypting the same password will create the same cipher-text; the cipher-text becomes the password.

- **Limit log-on attempts:** Organisations should limit the number of log-on attempts. Many operating systems can be configured to lock a user ID after a set number of failed log-on attempts. This helps to prevent guessing of authentication data.

- **Secure authentication data as it is entered in network:** Organisations should protect authentication data as it is entered into the IT system, including suppressing the display of the password as it is entered and orienting keyboards away from view.

- **Administer data properly:** Organisations should carefully administer authentication of data and tokens including procedures to disable lost or stolen passwords or tokens and monitoring systems to look for stolen or shared accounts.

■ **Passwords:** If passwords are used for authentication, organisations should consider following factors:

- **Specify the required password attributes:** Secure password attributes such as a minimum length, inclusion of special characters, not being in an online dictionary, and being unrelated to the user ID

should be specified and enforced.

- **Frequent change of password:** Passwords should be changed periodically. This considerably increases the security of an account / network.

- **User awareness:** User awareness should be created for not to use easy-to-guess passwords, not to divulge their passwords, and not to store passwords where others can find them.

- **Authentication Method:** Appropriate authentication methods are important at a minimum, however, centralised authentication methods are even better when either

  a) large numbers of users for devices are involved or,

  b) large numbers of devices are used in the network.

  Centralised authentication systems such as 'RADIUS' and 'Kerberos' manage centralised user account information so that the Remote Access Server (RAS) units, or other types of equipment, can access securely. These centralised schemes allow information to be stored in one place instead of many places. Instead of having to manage users on many devices, one location of user management can be used. If user information needs to be changed, such as a new password, one simple task can accomplish this. If a user leaves, the deletion of the user account prevents access for all equipment using centralised authentication. A typical problem with non centralised authentication in larger networks is remembering to delete accounts in all places. Centralised authentication systems such as RADIUS can usually be seamlessly integrated with other user account management schemes such as Active Directory or LDAP directories. This approach means that not only centralised authentication is being provided for the users of RAS and devices, but also the account information is unified with the domain accounts. Below figure shows a Windows Domain controller operating as both an Active Directory server and a RADIUS server for network elements to authenticate into an Active Directory domain.

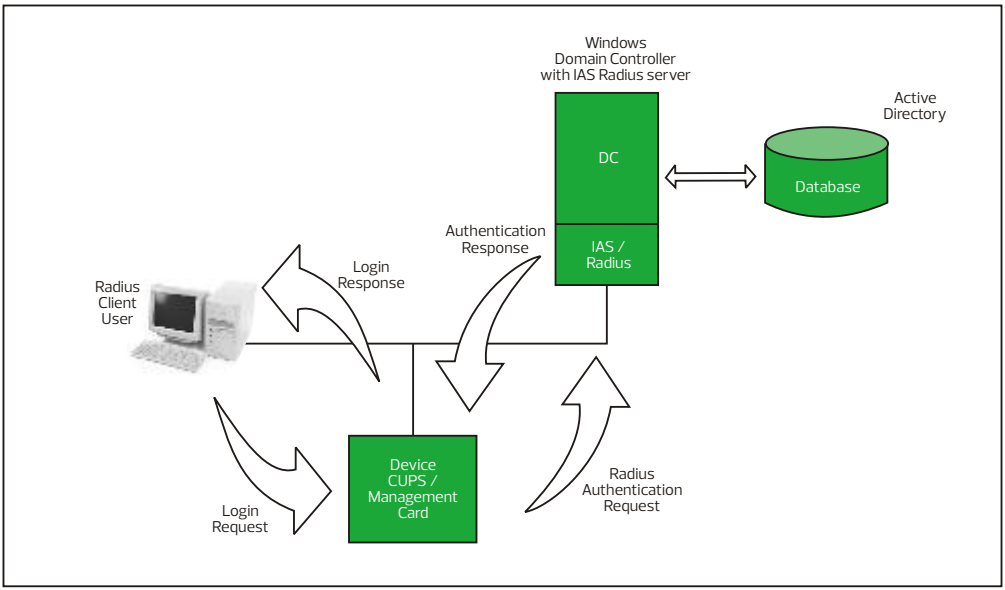


Figure 5 – Windows DC with RADIUS server for user authentication

3.2.2 Define Access Controls

Access is the ability to do something with a computer resource (e.g. use, change, or view.) Logical access controls are the system-based means by which the ability is explicitly enabled or restricted in some way. Logical access controls can prescribe not only who or what (e.g. in the case of a process) is to have access to a specific system resource but also the type of access that is permitted.

- **Access Criteria:** Organisations should control access to resources based on the following access criteria, as appropriate:
  - **Identity (user ID):** The identity is usually unique in order to support individual accountability, but it can be a group identification or even anonymous.
  - **Roles:** Access to information may also be controlled by the job assignment or function (i.e. the role) of the user who is seeking access. The process of defining roles should be based on a thorough analysis of how an organisation operates and should include input from a wide spectrum of users in an organisation.

- **Location:** Access to particular system resources may be based upon physical or logical location. Similarly, access to users can be restricted, based upon their network addresses (E.g., users from sites within the organisation may be permitted greater access than those from outside).

- **Time:** Time-of-day and day-of-week/month restrictions are another type of limitation on access. E.g., use of confidential personnel files may be allowed only during normal working hours.

- **Transaction:** These criteria can be used by organisations for handling transactions. E.g. Access to a particular account could be granted only for the duration of a transaction, say, in an account inquiry a caller would enter an account number and pin. A service representative would be given read access to that account. When completed, the access authorisation is terminated. This means that users (representative) do not have 'edit / write access' to such accounts to which they have access.

- **Service constraints:** Service constraints refer to those restrictions that depend upon the parameters that may arise during use of the application or that are pre-established by the resource owner/manager. E.g. A particular software package may be licensed by the organisation for only five users at a time. Access would be denied for a sixth user, even if the user were otherwise authorised to use the application. Another type of service constraint is based upon application content or numerical thresholds. E.g. an ATM machine may restrict transfers of money between accounts to certain limits or may limit maximum ATM withdrawals to INR 15,000 per day.

- **Access modes:** Organisations should consider the types of access, or access modes. The concept of access modes is fundamental to access control. Common access modes, which can be used in both operating and application systems, include read, write, execute, and delete. Other specialized accesses modes (more often found in applications) include 'create' or 'search'. Of course, these criteria can be used in conjunction with one another.

- **Access Control Mechanism:** An organisation should consider both, internal and external access control mechanisms. Internal access controls are a logical means of separating what defined users (or user groups) can or cannot do with system resources. External access controls are a means of controlling interactions between the system and outside people, systems, and services. When setting up access controls, organisations should consider the following mechanisms:

  - **Access Control Lists (ACLs):** ACLs are a register of users (including groups, machines, processes) who have been given permission to use a particular system resource and the types of access they have been permitted. These types of access lists serve as an important last defence and can be quite powerful on some devices with different rules for different access protocols.

  - **Constrained user interfaces:** Access to specific functions are restricted by never allowing users to request information, functions, or other resources for which they do not have access. Three major types exist: menus, database views, and physically constrained user interface, e.g., an ATM.

  - **Encryption and hashing:** Encrypted information can only be decrypted, and therefore read by those possessing the appropriate cryptographic key. While encryption can provide strong access control, it is accompanied by the need for strong key management. Encryption of data is usually accomplished by the combination of plaintext data (the input) with a secret key using a particular encryption algorithm (i.e. 3DES, AES, etc.). The result (output) is cipher-text. Unless someone (or a computer) has the secret key, they cannot convert the cipher-text back to plaintext.

    Another basic building block of cryptographic systems is the 'hash.' Hash methods take some plaintext input and perhaps key input and then compute a large number called a hash. This number is a fixed length (number of bits) regardless of the size of the input. Unlike the encryption methods that are reversible, where one can go back to plaintext with the key, hashes are one way. It is not mathematically

feasible to go from a hash back to plaintext. Hashes are used as special IDs in various protocol systems because they can provide a check mechanism on data similar to a CRC (cyclic redundant check) on a disk file to detect data alteration. The hashes are used as a data authentication method (different than user authentication). Anyone trying to secretly alter data in transit across a network will alter the hash values thus causing detection.

Table 1 – Majorly used cryptography algorithms

Algorithm	Primary Use	Protocol Uses
DES	Encryption	SSH, SNMPv3, SSL/TLS
3DES	Encryption	SSH, SNMPv3, SSL/TLS
RC4	Encryption	SSL/TLS
AES	Encryption	SSH, SSL/TLS
MD5	Hash	SSH, SNMPv3, SSL/TLS
SHA	Hash	SSH, SNMPv3, SSL/TLS

- **Port lockdown and minimizing running services:** Many network devices and computer hosts startup network services by default, each of these services could represent an opportunity for attackers, worms and Trojans. Very often all of these default services are not needed. Doing port lockdown by turning off services reduces this exposure.

- **Secure Gateways/Firewalls:** Secure gateways block or filter access between two networks, often between a private network and a larger, more public network such as the Internet or between different zones of private network such as LAN and DMZ (De-Militarized Zone). DMZ is used to provide secure access of public server of an organisation to public as well as internal users. Secure gateways allow internal users to connect to external networks while protecting internal systems from compromise. In most cases this means controlling the points of connectivity to the outside world, typically the Internet. Almost every medium and large-scale company has a

presence on the Internet and has an organisational network connected to it.

A firewall is a mechanism by which a controlled barrier is used to control network traffic into AND out of an organisational intranet. Firewalls are basically application specific routers. They run on dedicated embedded systems such as an internet appliance or they can be software programs running on a general server platform. More complex firewall rules can utilize what is called 'stateful inspection' techniques. This approach adds to the basic port blocking approach by looking at traffic behaviours and sequences to detect spoof attacks and denial of service attacks. The more complex the rules, the greater the required computing power of the firewall.

- **Host-based Authentication:** Host-based authentication grants access based upon the identity of the host originating the request, instead of the identity of the user making the request. Many network applications in use today use host-based authentication to determine whether access is allowed. Under certain circumstances, it is fairly easy to masquerade as the legitimate host, especially if the masquerading host is physically located close to the host being impersonated.

4.0

WIRELESS NETWORK SECURITY

Chapter 4: Wireless Network Security

IT departments of most of the businesses are largely adopting the Wi-Fi networks for better and easy access of network resources due to which an entirely new dimension of vulnerability and intruders is introduce to network security. As an extension of wired network, Wi-Fi provides easy access of applications and data for using mobile devices such as notebook PCs, mobiles and other handheld devices which help business to achieve better productivity and efficiency. Following are few common wireless threats which can affect the wireless security.

- **Rogue / Unauthorised Access Points:** The most common, as well as most dangerous, wireless threat is the rogue access point. The rogue access point is typically a low cost, SOHO-class access point brought in by an employee who wishes wireless access. The default access point settings typically have no security enabled, and thus when plugged into the corporate network create an entryway for anyone with a Wi-Fi client within range.

- **Incorrectly Configured Access Points (AP):** Incorrectly configured access points can be a threat to WLAN security. Many network administrators configure the AP in default mode with default SSID and password to broadcast the SSID and verify the authorised users. Broadcasting SSID can be a mistake, since it gives intruders to gain the SSID and can connect the internal or corporate network using the same. Authorised users may also hamper the integrity of the network by abusing the connection speeds or consuming complete bandwidth.

- **Rogue Ad-Hoc Network:** Similar to rogue access points, ad-hoc wireless network can also be a threat to the wireless LAN security without information of security managers. Wireless LAN cards can enable peer-to-peer networking between laptops without an access point. These ad hoc connections can transfer the corporate data to any unauthorised user without connecting to corporate network. While WLAN cards operate in ad hoc mode, any unauthorised station or user can connect directly to an authorised user and gain the access to the entire network because ad hoc network offers little or no authentication management.

- **Soft Access Points :** Wireless enabled laptops are easily configured to act as an access point with help of commonly available freeware tools. These laptops which act as an access point is known as soft AP pose all the risk like rouge access point by broadcasting an insecure connection to the corporate network.

- **Evil Twin Aps:** It is also known as fake wireless AP which is a wireless version of phishing attack. Fake Aps are configured by attacker to broadcast the same network name (SSID) as a legitimate business WLAN, causing nearby Wi-Fi clients to connect to them. Fake AP can be configured to monitor the user traffic and pass the traffic through the legitimated access point, or it can simply deny the access after getting authentication credentials. Most of the Evil twin attack is performed to gain the legitimate network user credentials.

- **Rogue Clients:** Rogue clients are those that are unauthorised to attach to an authorised corporate wireless network. This may occur through an authorised acces point that has been misconfigured with encryption turned off, or through an access point that has had its encryption/ authentication compromised and uses the key to connect to a properly configured authorised access point.

- **Denial of Service Attack:** Denial of service attack is a threat that can cause havoc on a large number of users simultaneously. There are various forms of wireless denial of service attacks, but they typically involve flooding a channel or channels with de-authentication or similar packets that terminate all current and attempted client associations to access points. Denial of service attacks can be particularly destructive to voice over Wi-Fi applications, completely halting the conversation.

How to Secure Wireless Network?

Securing a wireless LAN is not difficult – industry advances in technology and vendor innovation makes this easier than ever. Following are few factors can be considered for securing enterprise wireless LAN.

- **Change the manufacturer's default SSID to a 'Secure' SSID:** Access points

come with a standard network name such as tsunami, default, Linksys, etc., that broadcast to clients to advertise the availability of the access point. This should be changed / renamed immediately upon installation. While renaming the access point SSID, consider something which cannot be easily guessed or found on internet.

- **Strong Encryption and Authentication:** Default settings for most access points do not include any form of security being enabled. This is the most common reason that wireless LANs are hacked or used by unauthorised personnel. For enterprises, it is recommended that the most secure over-the-air encryption and authentication method be used – either WPA2 or WPA or a VPN.

  WPA2, also known as IEEE 802.11i when the access point is certified by the Wi-Fi Alliance, uses IEEE 802.1x for mutual authentication between the client and the network and AES for data encryption. Its predecessor was WPA, an interim form of security certified by the Wi-Fi Alliance. WPA also uses 802.1x for authentication, but TKIP for encryption. AES is considered the stronger encryption method compare to TKIP encryption. WPA2 and WPA require the use of a RADIUS server to provide the unique, rotating encryption keys to each client.

  If WPA2 or WPA cannot be used, a VPN is the next best solution for securing the over-the-air client connection. IPsec and SSL VPNs provide a similar level of security as WPA2 and WPA. Their downside for larger wireless LAN deployments is that all wireless LAN traffic must be funnelled to the VPN server, which may create a bottleneck. Also, latency sensitive applications such as wireless VoIP or Citrix may lose connectivity when roaming due to long latencies.

- **Use of Access Point with VLANs support:** Many different types of users may need to access the wireless LAN network. An access point that supports virtual LANs (VLANs) allows each authorised wireless LAN user to gain entry to only the network resources they need to access. As an example, personnel in shipping and manufacturing might access the wireless network using the SSID 'system_ops' which provides access only to email and ERP systems. Marketing and sales might access the wireless

network using the SSID 'business' which accesses customer and sales database information.

- **Secure WLAN Management Access:** The wireless LAN system should support secure and authenticated methods of management. Reconfiguring the access point through the management port is one method a malicious external user might try to access the corporate network. Wireless LAN systems should provide SNMPv3, SSH (secure Web), and SSH interfaces. Furthermore, the system should be configurable such that management is possible only from restricted stations/nodes on a specific VLAN which can modify the WLAN network settings.

- **Physically Secure the Access Points (Aps):** Access points should be secured against direct tampering or theft. If possible, access points should be deployed above a suspended ceiling so they are 'out of sight' and 'out of mind', with only the antenna visible. If this is not possible and the access points are physically accessible, management via a local serial port should be disabled or only available via secure access methods. Newer switch-based wireless LAN architectures may also provide additional protection by not storing any information locally in the access point, but keeping it centralized in the wireless switch which can be located in a secured wiring closet.

- **Physically Monitoring of Exterior Premises:** As access point signals extend beyond the perimeter of most buildings, it is possible for someone outside the facilities to connect internally while sitting in a parking lot or across the street. If security patrols or video surveillance is already in use, it may be desirable to alert security personnel to be aware of vehicles or people that seem to be loitering near the building for extended periods of time. In one publicized incident, this is how several hackers were caught trying to steal credit card information from a retail store over the wireless LAN network.

5.0 MAINTAINING NETWORK SECURITY

Chapter 5: Maintaining Network Security

Security must be maintained by organisation to protect the network or system from various existing and evolving threats and attacks. Network security should be a perpetual process. Risks change over time, and so should security. Following factors can be considered for maintaining the security of organisation's network and assets.

- **Intrusion Prevention System (IPS):** Intrusion Prevention is a technology that evaluates the characteristics of inbound and outbound network traffic and, when properly configured, blocks malicious activity based on patterns that are monitored at the network level. Intrusion signature database should be updated regularly.

- **Patch Management:** Always make sure all PCs or Server or other network systems are up-to date with operating system (OS) security patches. This helps prevent computer viruses and malware from exploiting system operating system and entering into corporate network.

- **Antivirus Protection:** In addition to OS patches, confirm that Antivirus and Malware protection is installed on all nodes or server and definitions are up to date. This further protects corporate PC from exploits and helps to maintain the network security.

- **User Awareness, Education and Training:** An awareness programme should aim to make employees and, where relevant, contractors aware of their responsibilities for network security or Data security and the means by which those responsibilities are discharged.

- **Logging and Monitoring:** Logging and monitoring are critical to detecting attacks on servers or other network assets and responding quickly. Logging is the act of recording key information about the server or network assets and services. The logs are generated by both operating system (event logs) and the applications. Logs can be useful in reconstruction of an attack or intrusion. However greatest benefit of logs is their use when monitoring the server or network assets.

  Monitoring is the periodic review of logs and other server information.

Monitoring is typically done continuously, hourly or daily. Regular monitoring identifies points of exposure and incidents of policy and procedural violation, which can then be acted upon.

Logging and monitoring are passive yet effective forms of intrusion detection. Continuous monitoring can increase the likelihood of detecting an attack against the network.

- **Regular Network Security Audit:** Security audit is a systematic evaluation of the security control by measuring how well it adapts to set of established benchmarks or organisation IT security policy. A thorough audit typically assesses the security of the system's physical configuration and environment, software, information handling processes and user practices. Network security audit review focuses on:

  — providing management with an independent assessment relating to the effectiveness of the network perimeter security and its alignment with the IT security architecture and policy

  — providing management with an evaluation of the IT function's preparedness in the event of an intrusion

  — identifying issues which affect the security of the enterprise's network

  Network security audit can also be performed as a part of the regulatory compliance audit that specifies how organisations must deal with the information and assets.

- **Regular Vulnerability Assessment:** Patch management and antivirus protection are basic in securing network. Vulnerability assessments are performed to determine the actual security posture of a network environment. Networks are a dynamic entity, they evolve and change constantly. A vulnerability assessment should be performed regularly and inform the responsible person or team every time change is detected to make the utmost of network security protection.

- **Regular Network Penetration Test:** A vulnerability assessment simply identifies and reports noted network vulnerabilities or loop holes, whereas a penetration test attempts to exploit the vulnerabilities to determine whether unauthorised access or other malicious activity is possible. Penetration testing typically includes network penetration testing and application security testing as well as controls and processes around the networks and applications, and should be performed from both outside the network trying to come in (external testing) and from inside the network. Penetration test confirms the exact level of impact or damage which can be made to network or system by simulating attacks from malicious outsiders who would not otherwise have authorised access to the network or as internal users.

Glossary

Terms	Definition
Access Control	Access Control ensures that resources are only granted to those users who are entitled to them.
Access Matrix	An Access Matrix uses rows to represent subjects and columns to represent objects with privileges listed in each cell.
Advanced Encryption Standard (AES)	An encryption standard being developed by NIST. Intended to specify an unclassified, publicly-disclosed, symmetric encryption algorithm.
Access Point (AP)	A wireless access point (AP) is a device that allows wireless devices to connect to a wired network using Wi-Fi, or related standards. The AP usually connects to a router (via a wired network) as a standalone device, but it can also be an integral component of the router itself.
Authenticity	Authenticity is the validity and conformance of the original information.
Authorization	Authorization is the approval, permission, or empowerment for someone or something to do something.
Backdoor	A backdoor is a tool installed after a compromise to give an attacker easier access to the compromised system around any security mechanisms that are in place.
Biometrics	Biometrics use physical characteristics of the users to determine access.
Cipher	A cryptographic algorithm for encryption and decryption
Ciphertext	Ciphertext is the encrypted form of the message being sent.
Client	A system entity that requests and uses a service provided by another system entity, called a "server." In some cases, the server may itself be a client of some other server.

Glossary

Terms	Definition
Data Encryption Standard (DES)	A widely-used method of data encryption using a private (secret) key. There are 72,000,000,000,000,000 (72 quadrillion) or more possible encryption keys that can be used. For each given message, the key is chosen at random from among this enormous number of keys. Like other private key cryptographic methods, both the sender and the receiver must know and use the same private key.
Demilitarized Zone (DMZ)	In computer security, in general a demilitarized zone (DMZ) or perimeter network is a network area (a subnetwork) that sits between an organisation's internal network and an external network, usually the Internet.
Domain Name	A domain name locates an organisation or other entity on the Internet.
Domain Name System (DNS)	The domain name system (DNS) is the way that Internet domain names are located and translated into Internet Protocol addresses. A domain name is a meaningful and easy-to-remember "handle" for an Internet address
Event	An event is an observable occurrence in a system or network.
Filter	A filter is used to specify which packets will or will not be used. It can be used in sniffers to determine which packets get displayed, or by firewalls to determine which packets get blocked
Firewall	A logical or physical discontinuity in a network to prevent unauthorised access to data or resources.
Gateway	A network point that acts as an entrance to another network.
Hardening	Hardening is the process of identifying and fixing vulnerabilities on a system.

Glossary

Terms	Definition
Incident	An incident as an adverse network event in an information system or network or the threat of the occurrence of such an event.
Incident Handling	Incident Handling is an action plan for dealing with intrusions, cyber-theft, denial of service, fire, floods, and other security-related events. It is comprised of a six step process: Preparation, Identification, Containment, Eradication, Recovery, and Lessons Learned.
Internet Control Message Protocol (ICMP)	An Internet Standard protocol that is used to report error conditions during IP datagram processing and to exchange other information concerning the state of the IP network.
Internet Protocol (IP)	The method or protocol by which data is sent from one computer to another on the Internet.
IP Address	A computer's inter-network address that is assigned for use by the Internet Protocol and other protocols. An IP version 4 address is written as a series of four 8-bit numbers separated by periods.
Kerberos	A system developed at the Massachusetts Institute of Technology that depends on passwords and symmetric cryptography (DES) to implement ticket-based, peer entity authentication service and access control service distributed in a client-server network environment.
Lightweight Directory Access Protocol (LDAP)	A software protocol for enabling anyone to locate organisations, individuals, and other resources such as files and devices in a network, whether on the public Internet or on a corporate Intranet.
Packet	A piece of a message transmitted over a packet-switching network. One of the key features of a packet is that it contains the destination address in addition to the data. In IP networks, packets are often called datagrams.

Glossary

Terms	Definition
Patch	A patch is a small update released by a software manufacturer to fix bugs in existing programs.
Patching	Patching is the process of updating software to a different version.
RADIUS Server	Remote Authentication Dial-In User Service (RADIUS) is a networking protocol that provides centralized Authentication, Authorization, and Accounting (AAA) management for users who connect and use a network service
Risk	Risk is the product of the level of threat with the level of vulnerability. It establishes the likelihood of a successful attack.
Risk Assessment	A Risk Assessment is the process by which risks are identified and the impact of those risks determined.
Router	Routers interconnect logical networks by forwarding information to other networks based upon IP addresses.
Secure Sockets Layer (SSL)	A protocol developed by Netscape for transmitting private documents via the Internet. SSL works by using a public key to encrypt data that's transferred over the SSL connection.
Server	A system entity that provides a service in response to requests from other system entities called clients.
Session	A session is a virtual connection between two hosts by which network traffic is passed.
Software	Computer programs (which are stored in and executed by computer hardware) and associated data (which also is stored in the hardware) that may be dynamically written or modified during execution.

Glossary

Terms	Definition
SSID	SSID is simply the technical term for a network name.
Switch	A switch is a networking device that keeps track of MAC addresses attached to each of its ports so that data is only transmitted on the ports that are the intended recipient of the data.
TCP/IP	A synonym for "Internet Protocol Suite;" in which the Transmission Control Protocol and the Internet Protocol are important parts. TCP/IP is the basic communication language or protocol of the Internet. It can also be used as a communications protocol in a private network (either an Intranet or an Extranet).
Threat	A potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm.
TKIP	Temporal Key Integrity Protocol, an encryption method used in Wi-Fi Protected Access (WPA), which replaced WEP in WLAN products
Transport Layer Security (TLS)	A protocol that ensures privacy between communicating applications and their users on the Internet. When a server and client communicate, TLS ensures that no third party may eavesdrop or tamper with any message. TLS is the successor to the Secure Sockets Layer.
Triple DES	A block cipher, based on DES, that transforms each 64-bit plaintext block by applying the Data Encryption Algorithm three successive times, using either two or three different keys, for an effective key length of 112 or 168 bits.
User	A person, organisation entity, or automated process that accesses a system, whether authorised to do so or not.

Glossary

Terms	Definition
VLAN	A VLAN is a group of devices on one or more LANs that are configured to communicate as if they were attached to the same wire, when in fact they are located on a number of different LAN segments. Because VLANs are based on logical instead of physical connections, they are extremely flexible.
Wireless Application Protocol (WAP)	A specification for a set of communication protocols to standardize the way that wireless devices, such as cellular telephones and radio transceivers, can be used for Internet access, including e-mail, the World Wide Web, newsgroups, and Internet Relay Chat.
Zombies	A zombie computer (often shortened as zombie) is a computer connected to the Internet that has been compromised by a hacker, a computer virus, or a trojan horse. Generally, a compromised machine is only one of many in a botnet, and will be used to perform malicious tasks of one sort or another under remote direction. Most owners of zombie computers are unaware that their system is being used in this way. Because the owner tends to be unaware, these computers are metaphorically compared to zombies.

References

https://www.sans.org/
https://en.wikipedia.org/wiki/Network_security
http://www.blackbox.com/
http://www.isaca.org/
http://csrc.nist.gov/publications/nistpubs/
http://www.ciscopress.com/
http://www.cisco.com/
http://windows.microsoft.com/
http://www.apc.com/
https://sophos.com/
http://networkworld.com/

NOTES

NOTES

RSM in India

Mumbai
13th Floor, Bakhtawar
229, Nariman Point
Mumbai – 400 021.

301-309, A Wing
3rd Floor, Technopolis Knowledge Park
Mahakali Caves Road, Andheri (E)
Mumbai – 400 093.

201, Shree Padmini
Teli Galli Junction
Andheri (E), Mumbai – 400 069.

New Delhi – NCR
2nd Floor, Tower-B
B-37, Sector-1
Noida – 201 301.

Chennai
Abhinav Centre
No. 4, Co-operative Colony
Off. Chamiers Road
Alwarpet, Chennai – 600 018.

1A, Chamiers Apartments
62/121, Chamiers Road
R. A. Puram, Chennai – 600 028.

Kolkata
A-6, 12th Floor
Chatterjee International Centre
33A, Jawaharlal Nehru Road
Kolkata – 700 071.

Bengaluru
Sujaya, No. 1007, 2nd Cross
13th Main, HAL II Stage
Bengaluru – 560 038.

Surat
DTA-2, G-02 to G-05 Plot
Gujarat Hira Bourse
Ichhapore-2
Surat – 394 510.

T-720, Belgium Tower
Opp. Linear Bus Stop
Ring Road, Surat – 395 002.

B/604-605, Tirupati Plaza
Athwa Gate, Nanpura
Surat – 395 001.

Hyderabad
217, Maruthi Corporate Point
Swapnalok Complex
92, Sarojini Devi Road
Secunderabad – 500 003.

Ahmedabad
B-504, Narnarayan Complex
Navrangpura
Ahmedabad – 380 009.

Pune
102, First Floor
Shree Residency
Baner Balewadi Road
Near Laxmi Mata Mandir
Balewadi, Pune – 411 045.

Gandhidham
Divyasarika, Plot No. 41
Ward 10-A, Gurukul
Gandhidham – 370 201.

Indore
106, Manas Bhavan Extension
1st Floor, R.N.T. Marg
Indore – 452 001.

Jaipur
346, 3rd Floor
Ganpati Plaza, M.I. Road
Jaipur – 302 001.

For further information please contact:

RSM Astute Consulting Pvt. Ltd.
13th Floor, Bakhtawar, 229, Nariman Point, Mumbai – 400 021.
T: (91-22) 6108 5555 / 6121 4444
F: (91-22) 6108 5556 / 2287 5771
E: emails@rsmindia.in
W: www.rsmindia.in

Offices: Mumbai, New Delhi-NCR, Chennai, Kolkata, Bengaluru (Bangalore), Surat, Hyderabad, Ahmedabad, Pune, Gandhidham, Indore and Jaipur.


facebook.com/RSMinIndia


twitter.com/RSM_India


linkedin.com/company/rsm-india