2021

Cyber Attacks and Counter Measures: User Perspective

Dr. Babasaheb Ambedkar Open University

Cyber Attacks and Counter Measures: User Perspective

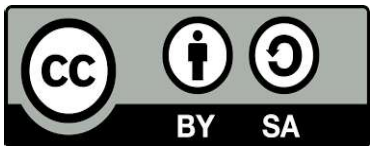
Course Writer

Mr. Rajendra Goswami	ICT Cell, Uttarakhand Open University, Haldwani
Er. Samarth Sharma	Security Consultant, Wipro Technologies, Bangalore
Er. Charanjeet Singh Chawla	Wing Commander, Indian Air Force, Ministry of Defence
Dr. Jeetendra Pande	Assistant Professor, School of CS & IT, Uttarakhand Open University, Haldwani
Chandrakant Mallick	Odisha State Open University, Sambalpur, Odisha
Bijay Kumar Paikaray	Centurion University of Technology and Management, Odisha
Guru Prasad Dash	Ravenshaw University, Cuttack, Odisha

Content Editor and Reviewer

Prof. (Dr.) Nilesh K. Modi	Professor & Director, School of Computer Science Dr.Babasaheb Ambedkar Open University, Ahmedabad

Acknowledgement: The content in this book is modifications based on the work created and shared by Uttarakhand Open University and Odisha State Open University for the subject Cyber Attacks and Counter Measures: User Perspective and Application Cyber Security used according to terms described in Creative Commons Attribution ShareAlike 4.0 International (CC BY-SA 4.0)



ISBN:

Printed and published by: Dr. Babasaheb Ambedkar Open University, Ahmedabad

Dr. Babasaheb Ambedkar Open University

PGDCS-204

Cyber Attacks and Counter Measures: User Perspective

Block-1:

Block-2:

Block-3:

Block-4:

Block-1

Unit 1: Cyber Attacks, Types of Attacks Motivation

1

Unit Structure

1.1 LEARNING OBJECTIVES

This unit purports at making you understand:

- What constitutes a cyber-attack,
- Types of cyber-attacks, and
- What motivates attacker(s) to do carry out attack(s).

1.2 INTRODUCTION

Everyone among us has one time or another has come across some form of attack. It could be physical or emotional or of some other kind. The intent is to cause some sort of harm – though sometimes it turn into a blessing in disguise. However, cyber attacks always aim at causing harm. They can be varied in their nature of approach and type of harm they inflict, depending on the motive, but the purpose is certainly malicious.

All of you must have encountered a situation when some unwanted changes, like installing some software or change your search engine, are made to your system or seen unwanted advertisements popping up while surfing Internet. These are examples of cyber attacks. These can range from being minor nuisance, like occasional popups, to creating havoc, like formatting hard disk.

1.3 CYBER ATTACK

Farhat et al[1] on 'What is a cyber attack' state as below:

A cyber attack is an attack initiated from a computer against a website, computer system or individual computer (collectively, a computer) that compromises the confidentiality, integrity or availability of the computer or information stored on it.

According to Anonymous[2], "Cyber-attack is any type of offensive maneuver employed by individuals or whole organizations that targets computer information systems, infrastructures, computer networks, and/or personal computer devices by various means of malicious acts usually originating from an anonymous

[1] http://www.hklaw.com/files/Publication/bd9553c5-284f-4175-87d2849aa07920d3/Presentation/PublicationAttachment/1880b6d6-eae2-4b57-8a97 9f4fb1f58b36/CyberAttacksPreventionand ProactiveResponses.pdf

[2] https://en.wikipedia.org/wiki/Cyber-attack

source that either steals, alters, or destroys a specified target by hacking into a susceptible system. These can be labeled as either a Cyber campaign, cyber warfare or cyber terrorism in different context. Cyber-attacks can range from installing spyware on a PC to attempts to destroy the infrastructure of entire nations."

In a nutshell, use of a device/system against another system/device with a malicious intent constitutes a cyber-attack.

1.4 TYPES OF CYBER ATTACK OR THREATS

Anonymous[3] gives a comprehensive list of cyber-attacks/threats which is reproduced below:

1. Backdoors – Backdoors[4] is bypassing normal authentication. Backdoor is a type of cyber threat in which the attacker uses a back door to install a key logging software, thereby allowing an illegal access to your system. This threat can turn out to be potentially serious as it allows for modification of the files, stealing information, installing unwanted software or even taking control of the entire computer.

   Default passwords can function as backdoors if they are not changed by the user. Some debugging features can also act as backdoors if they are not removed in the release version.

   Many computer worms, such as Sobig and Mydoom, install a backdoor on the affected computer (generally a PC on broadband running Microsoft Windows and Microsoft Outlook). Such backdoors appear to be installed so that spammers can send junk e-mail from the infected machines. Others, such as the Sony/BMG rootkit distributed silently on millions of music CDs through late 2005, are intended as DRM measures—and, in that case, as data gathering agents, since both surreptitious programs they installed routinely contacted central servers.

   A sophisticated attempt to plant a backdoor in the Linux kernel, exposed in November 2003, added a small and subtle code change by subverting the revision

[3] http://www.cybersecuritycrimes.com/types-of-cyber-attacks/

[4] https://en.wikipedia.org/wiki/Backdoor_(computing)

control system. In this case, a two-line change appeared to check root access permissions of a caller to the sys_wait4 function, but because it used assignment = instead of equality checking ==, it actually granted permissions to the system. This difference is easily overlooked, and could even be interpreted as an accidental typographical error, rather than an intentional attack.

In January 2014, a backdoor was discovered in certain Samsung Android products, like the Galaxy devices. The Samsung proprietary Android versions are fitted with a backdoor that provides remote access to the data stored on the device. In particular, the Samsung Android software that is in charge of handling the communications with the modem, using the Samsung IPC protocol, implements a class of requests known as remote file server (RFS) commands, that allows the backdoor operator to perform via modem remote I/O operations on the device hard disk or other storage. As the modem is running Samsung proprietary Android software, it is likely that it offers over-the-air remote control that could then be used to issue the RFS commands and thus to access the file system on the device.

2. Denial-of-Service Attack – A denial-of-service (DoS) attack is attacking the network to bring it down completely with useless traffic by affecting the host device which is connected to the Internet. DoS attack targets websites or services which are hosted on the servers. This type of attack can aim bank servers and credit card payment gateways.
3. Direct-access Attack – A direct-access attack simply means gaining physical access to the computer or its part and performing various functions or installing various types of devices to compromise security. The attacker can install software loaded with worms or download important data, using portable devices.
4. Eavesdropping – As the name suggests, eavesdropping means secretly listening to a conversation between the hosts on a network. There are various programs such as Carnivore and Narus Insight that can be used to eavesdrop.
5. Spoofing – Spoofing is a cyber attack where a person or a program impersonate another by creating false data in order to gain illegal access to a system. Such threats are commonly found in emails where the sender's address is spoofed.
6. Tampering – Tampering is a web based attack where certain parameters in the

URL are changed without the customer's knowledge; and when the customer keys in that URL, it looks and appears exactly the same. Tampering is basically done by hackers and criminals to steal the identity and obtain illegal access to information.

7. Repudiation Attack – A repudiation attack occurs when the user denies the fact that he or she has performed a certain action or has initiated a transaction. A user can simply deny having knowledge of the transaction or communication and later claim that such transaction or communication never took place.
8. Information Disclosure – Information disclosure breach means that the information which is thought to be secured is released to unscrupulous elements who are not trustworthy.
9. Privilege Escalation Attack – A privilege escalation attack is a type of network intrusion which allows the user to have an elevated access to the network which was primarily not allowed. The attacker takes the advantage of the programming errors and permits an elevated access to the network.
10. Exploits – An exploit attack is basically a software designed to take advantage of a flaw in the system. The attacker plans to gain easy access to a computer system and gain control, allows privilege escalation or creates a DOS attack.
11. Social Engineering – An attack by a known or a malicious person is known as social engineering. They have knowledge about the programs used and the firewall security and thus it becomes easier to take advantage of trusted people and deceive them to gain passwords or other necessary information for a large social engineering attack.
12. Indirect Attack – Indirect attack means an attack launched from a third party computer as it becomes more difficult to track the origin of the attack.
13. Computer Crime – A crime undertaken with the use of a computer and a network is called as a computer crime.
14. Malware – Malware refers to malicious software that are being designed to damage or perform unwanted actions into the system. Malware is of many types like viruses, worms, Trojan horses, etc., which can cause havoc on a computer's hard drive. They can either delete some files or a directory or simply gather data

without the actual knowledge of the user.

15. Adware – Adware is a software that supports advertisements which renders ads to its author. It has advertisements embedded in the application. So when the program is running, it shows the advertisement. Basically, adware is similar to malware as it uses ads to inflict computers with deadly viruses.
16. Bots – Bots is a software application that runs automated tasks which are simple and repetitive in nature. Bots may or may not be malicious, but they are usually found to initiate a DoS attack or a click fraud while using the internet.
17. Ransomware – Ransomware is a type of cyber security threat which will restrict access to your computer system at first and will ask for a ransom in order for the restriction to be removed. This ransom is to be paid through online payment methods only which the user can be granted an access to their system.
18. Rootkits – A rootkit is a malicious software designed in such a way that hides certain process or programs from normal anti-virus scan detection and continues to enjoy a privilege access to your system. It is that software which runs and gets activated each time you boot your system and are difficult to detect and can install various files and processes in the system.
19. Spyware – Spyware, as the name suggests, is a software which typically spies and gathers information from the system through a user's internet connection without the user's knowledge. A spyware software is majorly a hidden component of a freeware program which can be downloaded from the internet.
20. Scareware – Scareware is a type of threat which acts as a genuine system message and guides you to download and purchase useless and potentially dangerous software. Such scareware pop-ups seem to be similar to any system messages, but actually aren't. The main purpose of the scareware is to create anxiety among the users and use that anxiety to coax them to download irrelevant softwares.
21. Trojan Horses – Trojan Horses are a form of threat that are malicious or harmful codes hidden behind genuine programs or data which can allow complete access to the system and can cause damage to the system or data corruption or loss/theft of data. It acts as a backdoor and hence it is not easily detectable.

22. Virus – A computer virus is a self replicating program which, when executed, replicates or even modifies by inserting copies of itself into another computer file and infects the affected areas once the virus succeeds in replicating. This virus can be harmful as it spreads like wildfire and can infect majority of the system in no time.

23. Worm – Just like a virus, worm is a self replicating program which relies on computer network and performs malicious actions and spreads itself onto other computer networks. Worms primarily rely on security failures to access the infected system.

24. Phishing – Phishing is a cyber threat which makes an attempt to gain sensitive information like passwords, usernames and other details for malicious reasons. It is basically an email fraud where the perpetrator sends a legitimate looking email and attempts to gain personal information.

25. Identity Theft – Identity theft is a crime wherein your personal details are stolen and these details are used to commit a fraud. An identity theft is committed when a criminal impersonates individuals and use the information for some financial gain.

26. Intellectual Property Theft – Intellectual Property theft is a theft of copyrighted material where it violates the copyrights and the patents. It is a cybercrime to get hands onto some trade secrets and patented documents and research. It is basically a theft of an idea, plan and the methodology being used.

27. Password Attacks – Password attack is a form of a threat to your system security where attackers usually try ways to gain access to your system password. They either simply guess the password or use an automated program to find the correct password and gain an entry into the system.

28. Bluesnarfing – Bluesnarfing is a threat of information through unauthorized means. The hackers can gain access to the information and data on a Bluetooth enabled phone using the wireless technology of the Bluetooth without alerting the user of the phone.

29. Bluejacking – Bluejacking is simply sending of texts, images or sounds, to another Bluetooth enabled device and is a harmless way of marketing. However, there is a thin line between bluejacking and bluesnarfing and if crossed it results

into an act of threat.

30. DDoS – DDoS basically means a Distributed Denial of Service. It is an attempt to make any online service temporarily unavailable by generating overwhelming traffic from multiple sources or suspend services of a host connected to the internet.

31. Keylogger – A keylogger is a spyware that has the capability to spy on the happenings on the computer system. It has the capability to record every stroke on the keyboard, web sites visited and every information available on the system. This recorded log is then sent to a specified receiver.

1.5 MOTIVATION

Depending on the motivation, according to Ray[5], Verisign iDefense Security Intelligence Services classifies cyber-attacks into three categories: hacktivism, cyber crime and cyber- espionage.

Hacktivism is the act of hacking, or breaking into a computer system, for a politically or socially or ideologically motivated purpose. It is basically used as a means to promote an agenda. Hacktivists are responsible for denial-of-service (DoS), distributed denial of service (DDoS), information theft, data breaches, web site defacement, typosquatting(URL hijacking relying on typographical errors in URL spelling) and many other acts of digital sabotage.

Cyber crime, though, in a broad sense, covers any illegal activity that is committed through a digital means, here it refers to an activity with the monetary gain in mind. Such an activity can be a direct one, e.g., fraudulent bank transaction, or an indirect one, e.g., selling stolen

information in black market. Frequently used cyber crime tools are ATM and point-of-sale (PoS) skimming, RAM scrapping, code injection, key logging and phishing to extract confidential personal information.

Cyber espionage is unauthorized spying by computer[6]. However, a more

[5]http://www.circleid.com/posts/understanding_the_threat_landscape_cyber_attack_actors_and_motivations
[6]http://www.pcmag.com/encyclopedia/term/64376/cyber-espionage

comprehensive definition, and the associated tools, is given by Anonymous[7] which is as below:

Cyber spying, or cyber espionage, is the act or practice of obtaining secrets without the permission of the holder of the information (personal, sensitive, proprietary or of classified nature), from individuals, competitors, rivals, groups, governments and enemies for personal, economic, political or military advantage using methods on the Internet, networks or individual computers through the use of cracking techniques and malicious software including Trojan horses and spyware. It may wholly be perpetrated online from computer desks of professionals on bases in far away countries or may involve infiltration at home by computer trained conventional spies and moles or in other cases may be the criminal handiwork of amateur malicious hackers and software programmers.

John Arquilla (a US expert on national security affairs and defense analysis) added to new dimension to motivation behind cyber attacks by coining the term cyber warfare or cyber war. Cyber warfare has been defined as "actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption," but other definitions also include non-state actors, such as terrorist groups, companies, political or ideological extremist groups, hacktivists, and transnational criminal organizations[8].

The above definition of cyber espionage is very likely to raise some confusion as to whether it does not cover cyber war. It does not, which has been made clear by Anonymous[8] as below:

‘Cyber "war" is simply the act of fighting on an electronic battlefield with digital weapons. To attack an adversary’s capabilities in an effort to disable or destroy their ability to get things done. This may be completely digital in nature (such as communication and information systems) or the electronics that monitor and manage physical infrastructure, like power and water systems. Hostile code like StuxNet is an example of such weapons for cyber warfare.

Cyber "espionage" on the other hand is the act of obtaining information that is held in secrecy by the adversary. This in itself is not the end game - this information is

[7]https://en.wikipedia.org/wiki/Cyber_spying
[8]https://en.wikipedia.org/wiki/Cyberwarfare

then used for some sort of gain or strategic advantage. It must have an intrinsic value to the adversary, or its useless. In many cases, this may be to gain financial / competitive advantage in the business world, or strategic advantage over political communities of conflict.

Now here is where it gets complicated and is the source of much of the confusion. Cyber espionage is routinely used as a precursor to a cyber warfare strike. This allows an adversary to do reconnaissance in aid of an attack. In the movies, this would be sending in the recon patrol in the military to disable an enemy's capabilities before a major attack, or sending a spy into the enemy territory to gather intel before the strike. And this happens in the real world too.

Typically though cyber espionage is a covert operation that takes months or years to commit. It usually comes with signs of exfiltration and with the right tools can be tracked back to the source, with some level of certainty. Cyber warfare is different. The attack is usually pretty fast, striking in seconds and causing damage for use with other objectives.'

It must be noted that a perpetrator may belong to more than category of attack. For example, politically motivated cyber attacks may be carried out by members of extremist groups who use cyberspace to spread propaganda, attack websites, and steal money to fund their activities or to plan and coordinate physical-world crime[9].

The figure below shows worldwide motivation statistics, typically for April 2015. It clearly shows that most attacks (> 50%) fall under category 'cyber crime' whereas about one third belong to hacktivism. This is obvious from the fact that these two categories consist of mainly individuals and groups and require less resources whereas 'cyber espionage' and 'cyber warfare' usually require greater resources and, in many cases, government backing.

[9]https://en.wikipedia.org/wiki/Cyberwarfare

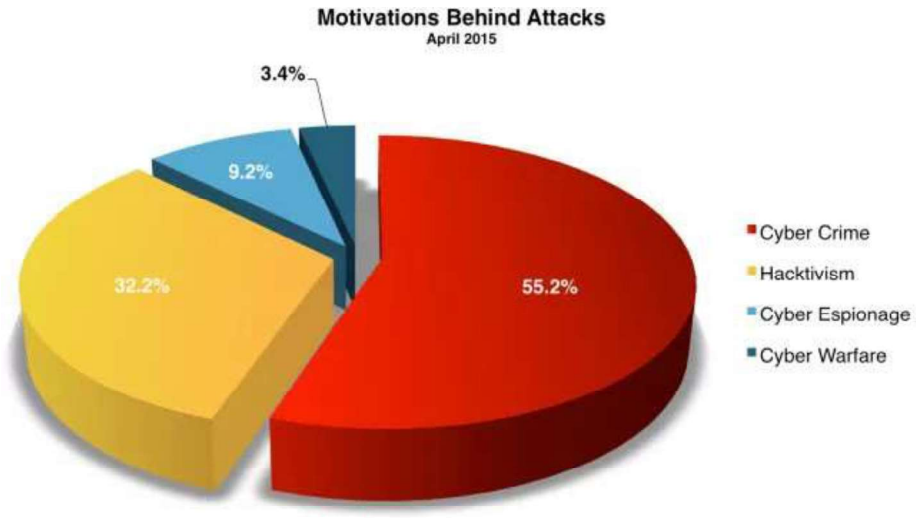


Figure 1: Motivation behind attacks[10]

1.6 LET US SUM UP

1 A **cyber attack** is an attack initiated from a computer against a website, computer system or individual computer (collectively, a computer) that compromises the confidentiality, integrity or availability of the computer or information stored on it.

2 **Hacktivism** is the act of hacking, or breaking into a computer system, for a politically or socially or ideologically motivated purpose.

3 **Cyber crime,** though, in a broad sense, covers any illegal activity that is committed through a digital means, here it refers to an activity with the monetary gain in mind.

4 **Cyber espionage** is unauthorized spying by computer.

5 **Cyber war** is simply the act of fighting on an electronic battlefield with digital weapons

[10]http://www.hackmageddon.com/category/security/cyber-attacks-statistics/

1.7 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. **Fill in the blanks:**

a. _____ is an attack initiated from a computer against a website, computer system or individual computer.

b. A_____is a spyware that has the capability to spy on the happenings on the computer system.

c. _____ is the act or practice of obtaining secrets without the permission of the holder of the information

d. _____is a threat of information through the hackers can gain access to the information and data on a Bluetooth enabled phone.

e. _____is a type of cyber security threat which will restrict access to your computer system at first and will ask for a ransom in order for the restriction to be removed.

Answers

a. Cyber attack
b. Keylogger
c. Cyber spying, or cyber espionage
d. Bluesnarfing
e. Ransomware

2. **State True or False:**

a. Hostile code like StuxNet is an example of weapons for cyber warfare.

b. Phishing is basically an email fraud where the perpetrator sends a legitimate looking email and attempts to gain personal information.

c. The ransom in Ransomware attack is to be paid through online payment methods.

d. In a privilege escalation attack URL are changed without the customer's knowledge.

e. Hacktivists are responsible for denial-of-service (DoS).

Answers

a. True
b. True
c. True

d. False
e. True

1.8 ASSIGNMENTS

1. What is Cyber Attack? How it is different from electronic authentication?
2. What are the different types of cyber attack?
3. Explain different types of Cyber Attacks in details.
4. What is Hacktivism?
5. Write a short note on Cyber War.
6. What is Cyber espionage?

1.9 ACTIVITIES

- Study about cyber-attacks happened during last five year globally.

Unit 2: Asset, Threat and Risk Management

2

Unit Structure

2.1 LEARNING OBJECTIVES

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

- Know Assets, classification of assets and protection of assets.
- Understand Vulnerability and Threat management
- Define Risk Management, Risk assessment, Risk treatment, Risk Mitigation

2.2 INTRODUCTION

Information security core objective is to secure the information asset of the organization. Loss of information can have severe impact over the economic condition of the organization along with the reputation loss in the market. It is a well-known fact that you cannot secure what you do not know exist in your environment. Asset management is all about discovery, ownership, value, acceptable use, protection, disposal of information related assets. Assets can be tangible and intangible. Examples of tangible assets are software and data while server is an example of tangible asset

The task of identifying assets that need to be secure is a less glamorous aspect of information security. But unless we know these assets, their locations and value, how are we going to choose the amount of time, effort or money that we should spend on safeguarding the assets? The major steps required for asset classification and controls are:

- Identification of the assets
- Accountability of assets
- Preparing a schema for information classification
- Implementing the classification schema

2.2.1 Identification of assets

What are the critical assets? Suppose your corporate office was devastated in a major fire. Surviving with this level of adversity will depend on what critical information you previously backed up at a remote location. Another terrifying scene is that a hacker hacked into your network and copied your entire customer

database. What impact will this have on your business?

Identifying the critical assets is important for many reasons. You will come to know what is critical and crucial for the business. You will be able to take suitable decisions regarding the level of security that should be provided to safeguard the assets. You will also be able to decide about the level of redundancy that is necessary by keeping an extra copy of the data or an extra server that you should procure and keep as a hot standby.

We should now focus on what is "Information Asset"? Is it hardware, software, program or database? We can broadly classify assets in the following categories:

2.2.1.1 Information assets

Every piece of information about your organization falls in this category. This information has been collected, classified, organized and stored in various forms.

i. Databases: Information about customer, production, finances and other different areas which are critical to the business. Confidentiality, Integrity and availability depends upon the classification by the data owner. Operational and support procedures: These have been developed over the years and provide detailed instructions on how to perform various activities.
ii. Archived information: Information of previous months or business cycles to maintain because of the law.

Continuity plans, fall-back arrangements: These plans are created to overcome any incident which can impact the business. Absence of these could result into the discontinuity of the business for a shorter or longer period depends upon the severity of the incident.

2.2.1.2. Software assets

These can be divided into two categories:

i. Application software: Application software implements business rules of the organization. Creation of application software is a time consuming

task. Integrity of application software is very important. Any flaw in the application software could impact the business adversely.

ii. System software: An organization would invest in various packaged software programs like operating systems, DBMS, development tools and utilities, software packages, office productivity suites etc.

Most of the software under this category would be available off the shelf, unless the software is obsolete or non-standard.

2.2.1.3 Physical assets

These are the visible and tangible equipment and could comprise of:

i. Computer equipment: Mainframe computers, servers, desktops and notebook computers.
ii. Communication equipment: Modems, routers, EPABXs and fax machines.
iii. Storage media: Magnetic tapes, disks, CDs and DATs.
iv. Technical equipment: Power supplies, air conditioners.
v. Furniture and fixtures

2.2.1.4 Services

Services that organization has outsourced to third party.

2.2.2 Accountability of assets

The next step is to create accountability of assets. This can be done easily for the tangible asset. A more difficult task is creating ownership for the information assets. There will be a number of users for these assets. But the prime responsibility for accuracy will lie with the asset owner. Any addition or modification to the information asset will only be done with the consent of the asset owner. For example, any changes to customer information will be done with the knowledge and consent of the marketing head. Information technology staff will probably make the changes, physically. But ownership clearly lies with the business head who has the prime responsibility for the content in the customer database.

Using these criteria, we have to identify the actual owners of each of the

information assets. This is also an important step for one more reason. Only an owner of the asset will be able to decide the business value of the asset. Unless the correct business value of the asset is known, we cannot identify the security requirement of the asset.

The next step is identifying owners of the application software. Application software implements the business rules. As such the business process owner should be the owner of application software. But the responsibility of maintaining application software to accurately reflect business rules will be vested with the application developers. As such, the accountability for application software should be with the application development manager.

System software ownership could be with the appropriate persons within the IT team. The owner of these assets will be responsible for maintaining all the system software including protecting the organization against software piracy.

2.2.2.1 Assets valuation

Another important task is to identify the value of the asset. Asset owner is the right person to verify the value of the asset. But the valuation of the information is a tedious task and depends on many factors which needs to be consider while evaluating them. We need to also consider the fact if in case information is not available how much it will going to impact our business. Also in case this information is leaked in market how it will going to impact the organization reputation in the market.

2.2.3 Preparing a schema for classification

The next important task is to create classification levels. The criteria for the classification of assets could be:

1. Confidentiality: Information comes under this criteria is highly important to the organization and only privileged employees should have access to it. Proper control should be put in place to control the access to this information.
2. Value: What is the asset value? Is it a high value item, costly to replace or a low value item?
3. Time: Is the information time sensitive? Will its confidentiality status change

after some time?

4. Access rights: Who will have access to the asset?
5. Destruction: How long the information will be stored? How can it be destroyed, if necessary?

Each asset needs to be evaluated against the above criteria and classified for easy identification. Let us look at each category for classification.

Confidentiality could be defined in terms of:

a. **Confidential**: Where the access is restricted to a specific list of people. These could be company plans, secret manufacturing processes, formulas, etc.
b. **Company only**: Where the access is restricted to internal employees only. These could be customer databases, manufacturing procedures, etc.
c. **Shared**: Where the resources are shared within groups or with people outside of the organization. This could be operational information and contact information like the internal telephone book to be shared with business partners and agents.
d. **Unclassified**: Where the resources are publicly accessible. For example, the company sales brochure and other publicity material.

Classification based on values could be high, medium or low value. Business justifications should be needed to support this classification. Criticality of the assets depends upon the impact it will create on the business. For example, a server who might not be very expensive but it can have the data which is very critical to the organization.

Access rights need to be defined for individuals by the owners. It depends on who is allowed to access the confidential information in the organization. Also who will approve to access those data in the organization?

Destruction of the information is a controlled activity. The information that is not required by the company any longer should be used by the competitor in the same business, that information should be destroyed by the pre-decided schedule and method depends on the confidentiality classification.

Classification schema should lead to an implementable structure. It should be simple to understand and identify.

2.2.4 Implementation of the classification schema

The real test of classification schema is when it is implemented. Information is a fluid resource. It keeps changing its form. The implementation should lead to a uniform way of identifying the information so that a uniform protection could be provided.

Let us take an example. A company's business plan is a confidential document. Let us trace its journey in the corporate world. The plan will be discussed behind closed doors, known to only a few senior members. In the next step the final plan will be prepared and stored on the MD's computer or that of his secretary. A soft copy of this plan would be sent by email to all executives who need to refer to it. The hard disk of every computer where the plan is stored will also have a backup copy on floppy or other media. Each member will no doubt print it and keep a hard copy folder for reference. An extra copy will also be prepared using the copying machine. If the email is not available, the plan would be sent by fax, post or courier.

So the 'confidential' plan is now distributed across the organization, available on the hard disks of computers belonging to each secretary and each senior executive. You get the general idea. If this can happen to confidential information, imagine how easy it is to get hold of other types of information. The information explosion has given rise to proliferation of information in every nook and corner of the organization.

A practical implementation of classification schema thus becomes very important. The classification label should not give an easy way of identification, which could be misused. It should provide the right amount of protection. In the example given above, each and every asset where the confidential information is residing or transiting through will have to be given the same classification level as that of the information itself. It may be desirable to altogether avoid transmission of confidential documents in soft copy format, for example as an attachment to email. Only a restricted number of hard copies should be circulated. If it is necessary to carry the soft copies, everyone should be

instructed to encrypt information for transmission and storage, and to memorize their passwords and keep them secret.

These frame works are used as plans or blueprints to design the security of an information security program to mitigate risk and bring down the impact of the risks under the acceptance criteria. Frameworks are often customized as per the requirement of the organizations. Framework assists enterprise to achieve their objectives and deliver values through effective governance and management.

2.3 VULNERABILITY AND THREATS

Information security vulnerabilities are weaknesses that expose an organization to risk. Vulnerability is a weakness in a system that could allow an attacker to compromise the security of the organization.

Vulnerability is a cyber-security term that refers to a flaw in a system that can leave it open to attack. Vulnerability may also refer to any type of weakness in a computer system itself, in a set of procedures, or in anything that leaves information security exposed to a threat.

Threats can exploit the vulnerabilities to impact the performance of the systems. A threat, in the context of information security, refers to anything that has the potential to cause serious harm to a system. Threats can include everything from viruses, Trojans, and back doors to outright attacks from hackers. A threat is something that may or may not happen, but has the potential to cause serious damage. Threats can lead to attacks on computer systems, networks and more.

The lack of access control in an office can be an example of vulnerability but unauthorized person who intentionally or unintentionally want to access the office premises will act as a threat which can exploit the absence of access control in the premises.

2.3.1 Types of threat

- **Physical damage**
  - fire
  - water
  - pollution
- **Natural events**
  - climatic
  - seismic
  - volcanic
- **Loss of essential services**
  - electrical power
  - air conditioning
  - telecommunication
- **Compromise of information**
  - eavesdropping,
  - theft of media
  - retrieval of discarded materials
- **Technical failures**
  - equipment
  - software
  - capacity saturation
- **Compromise of functions**
  - error in use
  - abuse of rights
  - denial of actions
- **Accidental**
  - equipment failure
  - software failure
- **Environmental**
  - natural event
  - loss of power supply

2.4 RISK MANAGEMENT

Risk management is an activity to manage the assessment, mitigation and monitoring of the risk in an organization. Information Security Risk Management is subset of the enterprise risk management. Information Security risk management access the risk which can impact the 'Confidentiality', 'Integrity' and 'Availability' of the organizational information. It also helps to identify the appropriate management actions and defined the priorities for implementing controls to protect those risks.

The risk management process help to create the organizational priorities and help organization to identify risk appetite for them. Top level management is authorized to make decisions about risk acceptance criteria.

Information security decisions should be managed by the top management. Only leadership of the organization should be able to decide the risk acceptance criteria because they are the stakeholders.

This process can be broadly divided into two components:

- Risk assessment
- Risk Mitigation

Risk assessment identifies, quantifies, and prioritizes risks against both criteria for risk acceptance and intents related to the organization. The assessment will result into the proper priorities of security risks and implementation of controls for securing those risks. The assessment result into determining of appropriate management actions and priorities for managing information security risks and for implementation of controls against them. The assessment helps to identify the impact of the risk. It also helps to identify the amount of resources needs to protect the assets. The scope of a risk assessment can be either whole organization, parts of the organization, and individual information system, or even specific system components or services. Performing risk assessment in a company infrastructure includes vulnerability assessment to help quantify risks. This process of assessing risks and helps to quantify them. This will also ensure that constantly evolving changes in security requirements and/or significant changes are assessed. For example, IT will be implementing new products or

service each year and new additional risk may be introduced due to vulnerabilities that can be exploited.

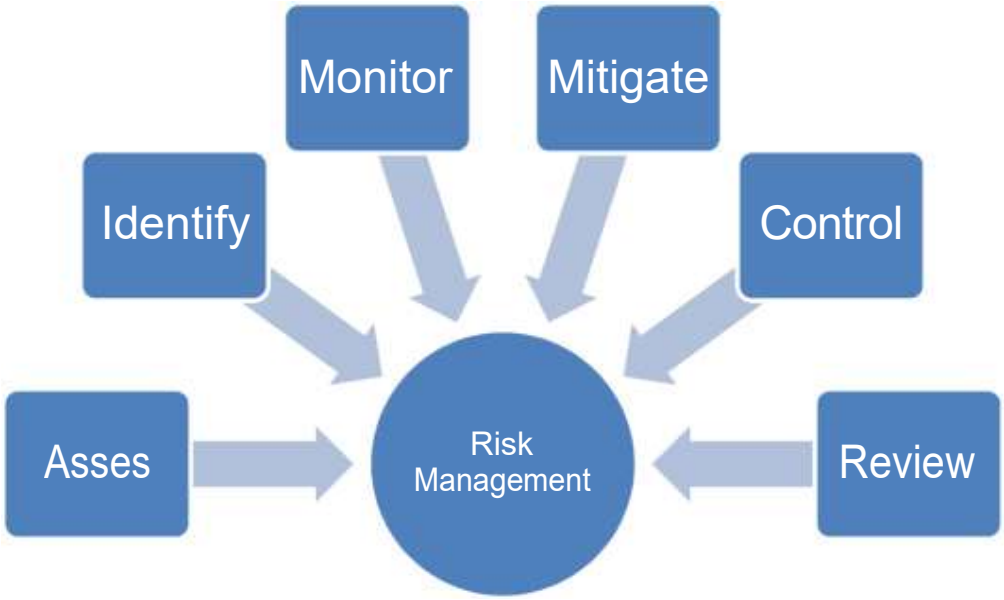


Figure 2: Risk management

Once a risk assessment is finished, risk treatment/risk mitigation is the next step in the process. For each of the risks identified during an assessment there should be a risk mitigation needs to be made. Risk mitigation is a systematic methodology used by senior management to reduce impact of the risk.

Risk mitigation can be completed through any of the following risk mitigation options:

- Risk Assumption: To accept the potential risk and continue operating the IT system or to implement controls to lower the risk to an acceptable level.
- Risk Avoidance: To avoid the risk by eliminating the cause or root cause of the system.
- Risk Limitation: To avoid the risk by eliminating the risk cause and/or consequence (e.g., for certain functions of the system or shut down the system when risks are identified)

Once a risk assessment is finished, risk treatment/risk mitigation is the next step in the process. For each of the risks identified during an assessment there should be a risk mitigation needs to be made. Risk mitigation is a systematic methodology used by senior management to reduce impact of the risk. Risk mitigation can be completed through any of the following risk mitigation options:

- Risk Assumption: To accept the potential risk and continue operating the IT system or to implement controls to lower the risk to an acceptable level.
- Risk Avoidance: To avoid the risk by eliminating the cause or root cause of the system.
- Risk Limitation: To avoid the risk by eliminating the risk cause and/or consequence (e.g., for certain functions of the system or shut down the system when risks are identified)
- Risk Planning: To manage risk by developing risk mitigation plan that prioritizes, implements, and maintains controls.
- Risk Transfer: To transfer the risk by using other options to compensate for the loss, such as purchasing insurance.

There are a variety of risk assessment tools and methodologies that can be used, but all are basically divided into quantitative and qualitative risk assessments.

2.4.1 Quantitative Risk Assessment

Quantitative risk assessments attempt to allocate a monetary value to the assets being measured, a monetary cost to the influence of an adverse event, and percentages to the frequency of threats and the likelihood of events. The monetary values and costs mentioned above are used to determine three elements needed to complete a quantitative risk assessment:

1. **Single Loss Expectancy (SLE):** What is the predictable loss from a single event? Consider physical destruction or theft of assets, loss of data, stopped or delayed processing, and interruption of business processes. Single-loss expectancy (SLE) is the monetary value predictable from the occurrence of a risk on an asset.

SLE = Asset Value x Impact (percent of asset loss incurred after an event)

2. **Annualized Rate of Occurrence (ARO):** How many times is an event expected to happen in a year?

For example, if insurance data suggests that a serious fire is likely to occur once in 25 years, then the annualized rate of occurrence is 1/25 = 0.04.

3. **Annual Loss Expectancy (ALO):** The annualized loss expectancy (ALE) is the product of the annual rate of occurrence (ARO) and the single loss expectancy (SLE).

ALO = SLE * ARO.

2.4.1.1 Advantages of Quantitative Risk Assessments

- Allows for a description and communication of consequences of event occurrence in monetary terms.
- It facilitates costs and benefits analysis for the selection of controls for the mitigation.

2.4.1.2 Disadvantages of Quantitative Risk Assessments

- It is very difficult in some cases to assign a dollar value to assets under the scope of the risk assessment. Especially in case information is under the scope of risk assessment as it is very difficult to identify the exact value of the information.
- Requires extensive time and staff resources.
- Values and costs are only as good and meaningful as the scope and accuracy of the amounts used to calculate them.
- Results of the assessment may be not exact and may be confusing.

2.4.2 Qualitative Risk Assessment

Qualitative risk assessments do not assign a financial value to the assets being measured, or to the impact of an adverse event. They measure the criticality of the assets and impact in range of high, low and medium. This ranking most parts comes under subjective:

- Low – Minor inconvenience tolerated for a short period of time.
- Medium — can result in destruction to the organization's assets which will require a moderate amount of time, effort, and money to repair.
- High— can result in loss of organization status. It will also result in a legal action or fine.

2.4.2.1 Advantages of Qualitative Risk Assessments

- Allows for ordering risks according to priority.
- Does not require extensive time and staff resources.
- It can recognize areas of greater risk in a short time and without significant expense.

2.4.2.2 Disadvantages of Qualitative Risk Assessments

- Results are estimates and subjective.
- Cost-benefit analysis during selection of mitigating controls is subjective.

2.5 LET US SUM UP

1. Asset management is all about discovery, ownership, value, acceptable use, protection, disposal of information related assets.
2. Information security vulnerabilities are weaknesses that expose an organization to risk. A vulnerability is a weakness in a system that could allow an attacker to compromise the security of the organization.
3. Threats can exploit the vulnerabilities to impact the performance of the systems. A threat, in the context of information security, refers to anything that has the potential to cause serious harm to a system.
4. Risk management is an activity to manage the assessment, mitigation and monitoring of the risk in an organization
5. The risk management process help to create the organizational priorities and help organization to identify risk appetite for them. Top level management is authorized to make decisions about risk acceptance criteria.
6. Risk assessment identifies, quantifies, and prioritizes risks against both criteria for risk acceptance and intents related to the organization.

7. Quantitative risk assessments attempt to allocate a monetary value to the assets being measured, a monetary cost to the influence of an adverse event, and percentages to the frequency of threats and the likelihood of events.
8. Qualitative risk assessments do not assign a financial value to the assets being measured, or to the impact of an adverse event.

2.6 ASSIGNMENTS

1. What is information asset?
2. How compromise of information asset impact the organization?
3. Explain the relation between threat and vulnerability?
4. Explain risk management?
5. Explain difference between qualitative and quantitative risk assessment?
6. Explain difference between ALO, ARO and SLE?
7. Explain the activities in risk assessment process?

Unit 3: Organization Security & Frameworks

3

Unit Structure

3.1 LEARNING OBJECTIVES

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

1. Information Security Frameworks
2. Types of framework and their advantage.
3. Organization structure, roles and responsibilities.
4. Overview of Policy, Procedures and Guidelines.

3.2 INTRODUCTION

Information security framework is a collection of documented procedures that are used to describe policies, procedures and guidelines around the implementation and management of Information security controls as per the security requirements of the enterprise requirements. These frame works are used as plans or blueprints to design the security of an information security program to mitigate risk and bring down the impact of the risks under the acceptance criteria. Frameworks are often customized as per the requirement of the organizations. Framework assist enterprise to achieve their objectives and deliver values through effective governance and management.

3.2.1 Advantage of Information Security framework

Framework helps in achieving organizational objective in a systematic and uniformed manner. Few main advantages of using information security framework is given below:

- Maintaining of processed information to support business decision.
- Achieving strategic objectives and provide benefit through effective use of resources.
- Maintain risk at acceptance level.
- Optimize the cost of IT services and technology.
- Supporting compliance with relevant laws, regulation, contractual agreement and policies.

3.2.2 Many Standards, Best Practices and Frameworks

In the coming section, we will see many profitable and non-profitable

organizations have made their own methodologies to security management, security control objectives, process management and enterprise management

Basic break of these standards, frameworks are given below:

Security Program Development

- **ISO/IEC 27000 series** developed by ISO and IEC for the development and management of ISMS.

Enterprise Architecture Development

- **Zachman framework** is developed by ZohnZazhman for the development of enterprise architectures.
- **TOGAF Model** developed by the open group for the enterprise architectures development.
- **MODAF Architecture** framework used mainly in military support missions developed by the British Ministry of Defense.

Security Enterprise Architecture Development

- **SABSA model**, Model and methodology for the development of information security enterprise architectures.
-

Security Controls Development

- **COBIT** Set of control objectives for IT management developed by Information Systems Audit and Control Association (ISACA) and the IT Governance Institute (ITGI)
- **SP 800-53Set** of controls to protect U.S. federal systems developed by the National Institute of Standards and Technology (NIST).

Corporate Governance

- **COSO** is a set of internal corporate controls to help decrease the risk of financial fraud developed by the Committee of Sponsoring Organizations (COSO) of the Treadway Commission.

Process Management

- **ITIL** Processes to permit for IT service management developed by the United Kingdom's Office of Government Commerce.
- **Six Sigma Business** management strategy that can be used to carry out process improvement.
- **Capability Maturity Model Integration (CMMI)** Organizational development for process improvement developed by Carnegie Mellon.

3.2.2.1 ISO 27001:2013

ISO 27001:2013, is an information security standard that was published in September'2013.It is revised version of ISO 27001: 2005, and is published by ISO (International Organization of Standards) and IEC(International Electrotechnical commission). This standard is specifically target to develop and maintain Information Security Management System in the organization. ISO 27001 gives the requirement for the implementation of ISMS (Information Security Management System).

Information Security Management System (ISMS) defines the control that need to be placed (configuration management, physical security management, data protection, auditing etc.) and explains how these should be treated during their whole lifecycle. ISMS provide a complete picture of the security by aligning and placing controls strategically in the organization. ISMS components should be integrated within the whole organization is should not be practiced in certain departments of the organization.

ISO 27001:2013 has 14 domains and 114 controls. Refer to ISO 27001:2013 to understand exactly the control structure. Due to intellectual property right we could list exact controls of ISO 27001:2013 but control structure and their purposes are given below:

1. **A.5 Information security policies –** It defines the control on how policies are documented and reviewed.
2. **A.6 Organization of information security –** It defines the control on the responsibilities given to different individuals.
3. **A.7 Human resources security –** It defines the control before the employment, during the employment and after employee left the organization.

4. **A.8 Asset management –** It defines the controls on information classification, media handling and inventory of assets.
5. **A.9 Access control –** It defines controls on accessing user access management, application, server and user responsibilities along with them.
6. **A.10 Cryptography –** It defines control related to encryption and decryption.
7. **A.11 Physical and environmental security –** It defines controls mentioning secure areas, access control for entrance and exit, equipment security, protection against threats, secure disposal, clear desk and clear screen.
8. **A.12 Operational security–** It defines controls related to change management, capacity management, backup, logging, monitoring, installation, vulnerabilities etc.
9. **A.13 Communications security–** It defines control related to network security, network services, transfer of information.
10. **A.14 System acquisition, development and maintenance –** It defines control for mentioning security requirement and development and support process.
11. **A.15 Supplier relationships –** It defines control on agreements controls on what to include in agreements, and how to monitor the suppliers
12. **A.16 Information security incident management –** It defines controls for reporting incidents, defining weakness, response procedure and collection of evidence.
13. **A.17 Information security aspects of business continuity management –** It defines the controls related to the plan of business continuity, procedures, verification and reviewing.
14. **A.18 Compliance –** It defines controls requiring the identifying applicable laws and regulation on intellectual property protection of personal data etc.

Table 1: Comparison of ISO 27001:2005 to ISO 27001:2013

Context	ISO 27001:2005	ISO 27001:2013
Process	The standard clearly states that it follows PDCA (Plan-Do-Check-Act) model.	The Standard does not mention any specific process model.
Risk Assessment	In ISO 27001:2005 asset owner determines how to treat the risk, accepting residual risk.	The Risk assessment and risk treatment plan process are aligned to ISO 31000.
Controls	There are 133 controls across 11 domains	There are 114 controls across 14 domains.
Documentation	Standard used records and documentation to cover all the requirements. Document include policies, procedure and guidelines. Records include audit, schedules etc.	There is no such distinction between control and records.

3.2.2.2 COSO

COBIT was derived from COSO framework which was developed by the Committee of Sponsoring Organizations of the Treadway Commission (COSO). In 1985, to deal with enterprise risk management, fraudulent activities, internal control and financial reporting. The COSO internal control framework comprises of five interconnected components derived from the way management manages a business. COSO assures that these components provide an effective framework for describing and evaluating According to COSO, these components provide an effective framework for describing and analyzing internal control system integrated in an organization. The five components are the following:

1. **Control environment:** The control environment sets the tone of an organization, influencing the control consciousness of its people. It is the foundation for all other components of internal control, providing discipline and structure. Control environment factors include the integrity, ethical values, management's operating style, delegation of authority systems, as well as the processes for managing and developing people in the organization.
2. **Risk assessment:** Every entity faces a variety of risks from external and internal sources that must be assessed. A precondition to risk assessment is establishment of objectives and thus risk assessment is the identification and analysis of relevant risks to the achievement of assigned objectives. Risk

assessment is a prerequisite for determining how the risks should be managed.

3 **Control activities:** Control activities are the policies and procedures that help ensure management directives are carried out. They help ensure that necessary actions are taken to address the risks that may hinder the achievement of the entity's objectives. Control activities occur throughout the organization, at all levels and in all functions. They include a range of activities as diverse as approvals, authorizations, verifications, reconciliations, reviews of operating performance, security of assets and segregation of duties.

4 **Information and communication:** Information systems play a key role in internal control systems as they produce reports, including operational, financial and compliance-related information that make it possible to run and control the business. In a broader sense, effective communication must ensure information flows down, across and up the organization. For example, formalized procedures exist for people to report suspected fraud. Effective communication should also be ensured with external parties, such as customers, suppliers, regulators and shareholders about related policy positions.

5 **Monitoring**: Internal control systems need to be monitored—a process that assesses the quality of the system's performance over time. This is accomplished through ongoing monitoring activities or separate evaluations. Internal control deficiencies detected through these monitoring activities should be reported upstream and corrective actions should be taken to ensure continuous improvement of the system.

The framework mentioned 17 principles associated with each components.

Table 2: COSO framework

Internal Control Component	**Principles**
Control environment	1. Demonstrate commitment to integrity and ethical values 2. Ensure that board exercises oversight responsibility 3. Establish structures, reporting lines, authorities and responsibilities 4. Demonstrate commitment to a competent workforce 5. Hold people accountable
Risk assessment	6. Specify appropriate objectives 7. Identify and analyze risks 8. Evaluate fraud risks 9. Identify and analyze changes that could significantly affect internal controls
Control activities	10. Select and develop control activities that mitigate risks 11. Select and develop technology controls 12. Deploy control activities through policies and procedures
Information and communication	13. Use relevant, quality information to support the internal control function 14. Communicate internal control information internally 15. Communicate internal control information externally
Monitoring	16. Perform ongoing or periodic evaluations of internal controls (or a combination of the two) 17. Communicate internal control deficiencies

There are certain limitation as Framework recognize that as internal control provide assurance of achieving the organizations objective, but limitation do exist as internal control do not overcome bad judgments, external events etc. which can cause failing of achieving its operational goal. Organization can face the failure from multiple factors:

- Breakdown due to human failures.
- Cases in which management override internal control.
- External event beyond the organizations control.
- Mistakes due to human intervention.

3.2.2.3 COBIT (IT Governance Framework)

Before understand the COBIT framework we need to understand use and motive of IT governance frameworks. IT governance is a management initiative to develop a structured framework which allow organization to align the IT with

the business goals while reducing risk and improving continually. IT governance is a top down approach which require strong management support to be successful in the organization. IT Governance focuses majorly on five areas given below:

1 Strategic alignment emphases on guaranteeing the linkage of business and IT plans; describing, maintaining and validating the IT value; and aligning IT operations with enterprise goals.

2 Value delivery is about accomplishing the value proposition throughout the delivery cycle, confirming that IT delivers the promised benefits against the strategy, focused on optimizing costs and proving the value of IT.

3 Resource management is about the optimum investment in, and the appropriate management of, critical IT resources: applications, information, infrastructure and people.

4 Risk management needs risk awareness by senior officers, a clear picture of the enterprise's acceptance of the risk, understanding of compliance and technical requirements.

5 Performance measurement monitors strategy implementation, project completion, resource usage, process performance and service delivery, using balanced scorecards that translate strategyinto action to achieve goals.

COBIT (Control objective for information and related technology) is a framework for developing, implementing, monitoring and improving Information technology governance and management practices. The COBIT framework is published by ISACA in 1996. The framework support organization governance by aligning IT goals with business goals. It helps enterprise to drive optimal value from IT by maintaining balance between resources use, benefits and optimizing risk levels. Adoption of COBIT will allow the organization to achieve the following goals:

- Alignment of IT with the business goals.
- Increased the importance of IT to business.
- Risk reduction.
- Continual improvement of IT.
- Development of goals and scorecards for measurement of IT in a structured

way.

COBIT has 5 key principles:

- Principle 1: Meeting Stakeholders Needs.
- Principle 2: Covering the enterprise end to end.
- Principle 3: Applying a single, integrated framework.
- Principle 4: enabling a Holistic approach.
- Principle 5: Separating governance from management.

Table 3: Differences between COSO and COBIT

COSO	COBIT
COSO is a model for cooperate governance.	COBIT is a model for IT governance.
COSO deals more at strategic level.	COBIT focuses more at operational level.

3.3 POLICIES, STANDARDS, BASELINES, GUIDELINES AND PROCEDURES

3.3.1 Security Policy

A Security policy is a statement given by the top management that reflects the role of security in the organization. It can be organizational policy, issue related policy or specific system related policy. Organization Security policy defines how the organization security program will be executed, program goals, roles and responsibilities and outlines how enforcement should be carried out. The organization security policy outlines how all security related activities will be carried out in the organization.

Organization security policy should have several important characteristic that should be understood and implemented:

- Policy should be aligned with the business objective, business should not be aligned with the policy.
- It should be easily understood document that is used as a reference point for all employee and management.
- It should be used to induce security into the business functions.
- It should be changed with any business function such as merger with the new company, adoption of new technology or change of

management/ownership.

- It should be tracked through version control.
- It should have clear and declarative statements.
- It should be reviewed on regular basis.

The Types of policies are given below:

1 **Regulatory** This type of policy ensures that the organization is following standards set by specific industry regulations (HIPAA, GLBA, SOX, PCI-DSS, etc.). It is very detailed and specific to a type of industry. It is used in financial institutions, healthcare facilities, public utilities, and other government-regulated industries.

2 **Advisory** This type of policy strongly advises employees as to which types of behaviors and activities should and should not take place within the organization. It also outlines possible ramifications if Employees do not comply with the established behaviors and activities. This policy type can be used, for example, to describe how to handle medical or financial information.

3 **Informative** This type of policy informs employees of certain topics. It is not an enforceable policy, but rather one that teaches individuals about specific issues relevant to the company. It could explain how the company interacts with partners, the company's goals and mission, and a general reporting structure in different situations.

A common hierarchy of security policies is outlined here:

- Organizational policy
- Acceptable use policy
- Risk management policy
- Vulnerability management policy
- Data protection policy
- Access control policy
- Business continuity policy
- Log aggregation and auditing policy
- Personnel security policy
- Physical security policy
- Secure application development policy

- Change control policy
- E-mail policy
- Incident response policy

3.3.2 Guidelines

Guidelines are recommended actions and operational instructions to users, IT staffs, where specific standard does not apply. A guideline is used to determine the course of action according to a set routine. Guidelines are the best practices used to achieve the goals mentioned in the security policy.

3.3.3 Procedure

Procedure are detailed step-by-step that should be accomplished to reach a certain goal. This apply to IT staff, Information security group members and others who need to carry out specific tasks. Procedures are at the lower level where in the documentation series because they are near to the computers and users. They provide detailed steps for configuration.

Procedure practically shows how policy, procedure and guidelines are actually implemented in the practical scenario. If policy states that password should be alpha numeric then procedure specifically explains how to configure the same on the systems.

3.4 LET US SUM UP

1. ISO 27001:2013 is a standard which explain the requirement to implement Information Security Management System.
2. Information security framework is a collection of documented procedures that are used to describe policies, procedures and guidelines around the implementation and management of Information security controls as per the security requirements of the enterprise requirements.
3. Frameworks are used to provide a structural approach to implement security in a systematic approach.
4. IT governance is a management initiative to develop a structured framework which allow organization to align the IT with the business goals while

reducing risk and improving continually.

5. COBIT is derived from the COSO framework
6. COSO deal with enterprise risk management, fraudulent activities, internal control and financial reporting.
7. A Security policy is a statement given by the top management that reflects the role of security in the organization. It can be organizational policy, issue related policy or specific system related policy.
8. Procedure are detailed step-by-step that should be accomplished to reach a certain goal. This apply to IT staff, Information security group members and others who need to carry out specific tasks.
9. Guidelines are recommended actions and operational instructions to users, IT staffs, where specific standard does not apply. A guideline is used to determine the course of action according to a set routine.
10. The survival and integrity of any given network infrastructure of any company or organization strongly depends on the application of computer forensics.

3.5 ASSIGNMENTS

1. What is Information Security Management System?
2. What is difference between ISO 27001:2005 and ISO 27001:2013?
3. Explain 5 components of COSO framework?
4. What is major difference between COSO and COBIT?
5. Explain the 5 focus areas on which IT governance focuses?
6. Explain difference between policy, procedure and guidelines

Block-2

Unit 1: Security Controls 1

Unit Structure

1.1. LEARNING OBJECTIVES

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

- Know security basics
- Implement physical controls
- Define access control models
- Understand desktop security
- Implement password security

1.2. INTRODUCTION

Securing the modern business network and IT infrastructure demands an end-to-end approach and a firm grasp of vulnerabilities and associated protective measures. While such knowledge cannot thwart all attempts at network incursion or system attack, it can empower network engineers to eliminate certain general problems, greatly reduce potential damages, and quickly detect breaches. With the ever-increasing number and complexity of attacks, vigilant approaches to security in both large and small enterprises are a must. Prior to discussing Procedural / People security controls we will start by defining security controls in general.

Security Controls are safeguards or countermeasures to avoid, detect, counteract, or minimize security risks to physical property, information, computer systems, or other assets. Controls help to reduce the risk of damage or loss by stopping, deterring, or slowing down an attack against an asset.

People are truly the weakest link in any security schema. Most people are not careful about keeping secrets such as passwords and access codes that form the basis for most secure systems. All security systems rely on a set of measures employed to control access, verify identity and protect disclosure of sensitive information. These measures usually involve one or more “secrets”. Should a secret be revealed or stolen then the systems that are protected by these secrets can be compromised. It may seem like a terribly obvious statement, but most systems are compromised in very basic ways. Leaving a

Post-It note with a system password stuck to the side of a computer monitor may seem foolish, but many people in fact do such things. Another example, which is only slightly less obvious, is the tendency to leave factory default passwords in certain network devices. One such device might be a network management interface to a UPS. UPS systems, whether small in capacity or large enough to power 100 servers, are often overlooked in a security scheme. If such devices are left with default usernames and passwords, it could just be a matter of time before someone gains access knowing nothing more than the device type and its published default credentials. Imagine a server bank with rock solid security protocols on each web and mail server crashed by a simple power cycle on an unprotected UPS!

The control environment sets the tone of an organization, influencing the control consciousness of its people. It is the foundation for all other components of internal control, providing discipline and structure. Control environment factors include the integrity, ethical values, and competence of the entity's people; management's philosophy and operating style; and the way management assigns authority and organizes and develops its people.

1.3. SECURITY BASICS

It is not possible to protect anything unless one clearly understands WHAT one wants to protect. Organizations of any size should have a set of documented resources, assets and systems. Each of these elements should have a relative value assigned in some manner as to their importance to the organization. Examples of things that should be considered are servers, workstations, storage systems, routers, switches, hubs, network and Telco links, and any other network elements such as printers, UPS systems and HVAC systems. Other important aspects of this task include documenting equipment location and any notes on dependencies. For instance most computers will rely on power backup systems such as UPSs which themselves may be part of the network if they are managed. Environmental equipment such as HVAC units and air purifiers may also be present.

The next step is to identify the potential "threats". Threats can come from both