PAPER NO. CT 61
SECTION 6

CERTIFIED
INFORMATION COMMUNICATION TECHNOLOGISTS
(CICT)

SYSTEM SECURITY

STUDY TEXT

www.masomonsingi.co.ke

KASNEB SYLLABUS

PAPER NO.16 SYSTEMS SECURITY

GENERAL OBJECTIVE

This paper is intended to equip the candidate with the knowledge, skills and attitude thatwill enable him/her to secure lCT systems in an organization

LEARNING OUTCOMES

A candidate who passes this paper should be able to:
• Identify types of threats to ICT systems
• Adopt different security mechanisms
• Prepare business continuity planning (BCP) strategies
• Develop and implement a systems security policy
• Undertake basic computer forensic audits
• Demonstrate social-ethical and professional values in computing.

CONTENT

1. Introduction to systems security

- Overview of systems security
- Goals of system security
- Security core concepts
- Security mechanisms

2. Security threats and controls

- Sources of threats
- Types of threats
- Crimes againstlCT and computer criminals
- Controlling security threats
- Ethical hacking

3. Systems security

- Classification
- People errors
- Procedural errors
- Software errors
- Electromechanical problems
- Dirty data

4. Physical and logical security

- Physical security
- Logical security (authentication, access rights. Others)

5. Data/software security

- Use of the normal security systems
- Vulnerability assessment

www.masomomsingi.co.ke

- Employing virus security precautions
- Employing Internet security precautions
- Vetting of ICT employees

6. Transmission security

- Symmetric encryption
- Asymmetric encryption
- Duplicate and alternate routing
- Firewall types and configuration
- Secure socket layer and transport layer security
- IPv4 and 1Pv6 security
- Wireless network security
- Mobile device security
- Wireless protected access

7. ICT risk management

- Risk management concepts
- Risk analysis
- Risk assessment framework
- Countermeasures
- Corporate risk document

8. Business continuity planning (BCP)

- BCP scope, teams and roles
- Backup types and strategies
- Hot and cold sites
- Disaster recovery plans

9. System security policy implementation

- Components of systems security policy
- Systems security policy development
- System security policy implementation
- Systems security strategies
- Audit

10. Introduction to computer forensics

- Computer forensics concepts
- Incidence handling
- Investigating desktop incidents
- Investigating network incidents
- Securing and preserving evidence

11. Professional values and ethics in computing

- Intellectual property and fraud
- Information systems ethical and social concerns
- Telecommuting and ethical issues of the worker
- Codes of ethics for IT professionals
- Professional ethics and values on the web and Internet

www.masomomsingi.co.ke

- Objectivity and integrity in computing
- The role of professional Societies in enforcing professional standards in Computing

12. **Emerging Issues and trends**

CONTENT **PAGE**

www.masomomsingi.co.ke

TOPIC 1

INTRODUCTION TO SYSTEMS SECURITY

Overview of systems security

Information security, sometimes shortened to **InfoSec**, is the practice of defending information from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction. It is a general term that can be used regardless of the form the data may take (e.g. electronic, physical).

Overview

IT security

Sometimes referred to as computer security, Information Technology security is information security applied to technology (most often some form of computer system). It is worthwhile to note that a computer does not necessarily mean a home desktop. A computer is any device with a processor and some memory. Such devices can range from non-networked standalone devices as simple as calculators, to networked mobile computing devices such as smartphones and tablet computers. IT security specialists are almost always found in any major enterprise/establishment due to the nature and value of the data within larger businesses. They are responsible for keeping all of the technology within the company secure from malicious cyber-attacks that often attempt to breach into critical private information or gain control of the internal systems.

Information assurance

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

Threats

Computer system threats come in many different forms. Some of the most common threats today are software attacks, theft of intellectual property, identity theft, theft of equipment or information, sabotage, and information extortion. Most people have experienced software attacks of some sort. Viruses, worms, phishing attacks, and Trojan horses are a few common examples of software attacks. The theft of intellectual property has also been an extensive issue for many businesses in the IT field. Intellectual property is the ownership of property usually consisting of some form of protection. Theft of software is probably the most common in IT businesses today. Identity theft is the attempt to act as someone else usually to obtain that person's personal information or to take advantage of their access to vital information. Theft of equipment or information is becoming more prevalent today due to the fact that most devices today are mobile. Cell phones are prone to theft and have also become far more desirable as the amount of data

www.masomomsingi.co.ke

capacity increases. Sabotage usually consists of the destruction of an organization′s website in an attempt to cause loss of confidence to its customers. Information extortion consists of theft of a company′s property or information as an attempt to receive a payment in exchange for returning the information or property back to its owner. There are many ways to help protect yourself from some of these attacks but one of the most functional precautions is user carefulness.

Governments, military, corporations, financial institutions, hospitals and private businesses amass a great deal of confidential information about their employees, customers, products, research and financial status. Most of this information is now collected, processed and stored on electronic computers and transmitted across networks to other computers.

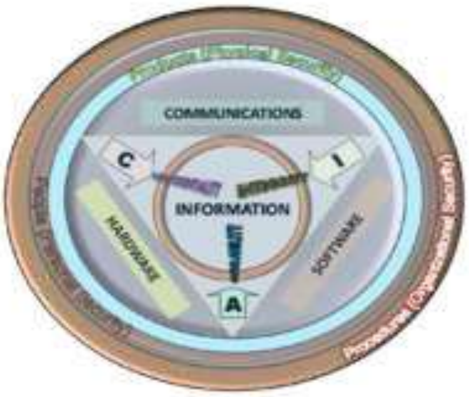
Should confidential information about a business' customers or finances or new product line fall into the hands of a competitor or a black hat hacker, a business and its customers could suffer widespread, irreparable financial loss, as well as damage to the company's reputation. Protecting confidential information is a business requirement and in many cases also an ethical and legal requirement. Hence a key concern for organizations today is to derive the optimal information security investment. The renowned Gordon-Loeb Model actually provides a powerful mathematical economic approach for addressing this critical concern.

For the individual, information security has a significant effect on privacy, which is viewed very differently in different cultures.

The field of information security has grown and evolved significantly in recent years. There are many ways of gaining entry into the field as a career. It offers many areas for specialization including securing network(s) and allied infrastructure, securing applications and databases, security testing, information systems auditing, business continuity planning and digital forensics.

omonsingi.co.ke

Definitions



Information Security Attributes: or qualities, i.e., Confidentiality, Integrity and Availability (CIA). Information Systems are composed in three main portions, hardware, software and communications with the purpose to help identify and apply information security industry standards, as mechanisms of protection and prevention, at three levels or layers: physical, personal and organizational. Essentially, procedures or policies are implemented to tell people (administrators, users and operators) how to use products to ensure information security within the organizations.

The definitions of InfoSec suggested in different sources are summarized below (adopted from).

1. "Preservation of confidentiality, integrity and availability of information. Note: In addition, other properties, such as authenticity, accountability, non-repudiation and reliability can also be involved." (ISO/IEC 27000:2009)

2. "The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability." (CNSS, 2010)

3. "Ensures that only authorized users (confidentiality) have access to accurate and complete information (integrity) when required (availability)." (ISACA, 2008)

4. "Information Security is the process of protecting the intellectual property of an organisation." (Pipkin, 2000)

5. "...information security is a risk management discipline, whose job is to manage the cost of information risk to the business." (McDermott and Geer, 2001)

6. "A well-informed sense of assurance that information risks and controls are in balance." (Anderson, J., 2003)

7. "Information security is the protection of information and minimizes the risk of exposing information to unauthorized parties." (Venter and Eloff, 2003)

8. "Information Security is a multidisciplinary area of study and professional activity which is concerned with the development and implementation of security mechanisms of all available types (technical, organisational, human-oriented and legal) in order to keep information in all its locations (within and outside the organization‘s perimeter) and, consequently, information systems, where information is created, processed, stored, transmitted and destroyed, free from threats.

www.masomomsingi.co.ke

THIS IS A SAMPLE
COMPLETE NOTES ARE IN SOFT AND IN HARD COPY
CALL|TEXT|WHATSAPP 0728 776 317
OR
Email: info@masomomsingi.co.ke

TOPIC 2

SECURITY THREATS AND CONTROLS

Threats classification

Threats can be classified according to their type and origin:

- Type 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
- Origin of threats
    - Deliberate: aiming at information asset
        - spying
        - illegal processing of data
    - accidental
        - equipment failure
        - software failure
    - environmental
        - natural event
        - loss of power supply
    - Negligence: Known but neglected factors, compromising the network safety and sustainability.

Note that a threat type can have multiple origins.

www.masomomsingi.co.ke

Threat model

People can be interested in studying all possible threats that can:

- affect an asset,
- affect a software system
- are brought by a threat agent

Threat classification

Microsoft has proposed a threat classification called STRIDE, from the initials of threat categories:

□ **S**poofing **of** user identity
□ **T**ampering
□ **R**epudiation
- **I**nformation disclosure (privacy breach or Data leak)

□ **D**enial of Service **(D.o.S.)**
□ **E**levation of privilege

Microsoft used to risk rating security threats using five categories in a classification called DREAD: Risk assessment model. The model is considered obsolete by Microsoft. The categories were:

- **D**amage – how bad would an attack be?
- **R**eproducibility – how easy it is to reproduce the attack?
- **E**xploitability – how much work is it to launch the attack?
- **A**ffected users – how many people will be impacted?
- **D**iscoverability – how easy it is to discover the threat?

The DREAD name comes from the initials of the five categories listed.

Associated terms

Threat agents or actors

Threat agents
Individuals within a threat population; practically anyone and anything can, under the right circumstances, be a threat agent – the well-intentioned, but inept, computer operator who trashes a daily batch job by typing the wrong command, the regulator performing an audit, or the squirrel that chews through a data cable.

www.masomomsingi.co.ke

Threat agents can take one or more of the following actions against an asset

- Access – simple unauthorized access
- Misuse – unauthorized use of assets (e.g., identity theft, setting up a porn distribution service on a compromised server, etc.)
- Disclose – the threat agent illicitly discloses sensitive information
- Modify – unauthorized changes to an asset
- Deny access – includes destruction, theft of a non-data asset, etc.

It‘s important to recognize that each of these actions affects different assets differently, which drives the degree and nature of loss. For example, the potential for productivity loss resulting from a destroyed or stolen asset depends upon how critical that asset is to the organization‘s productivity. If a critical asset is simply illicitly accessed, there is no direct productivity loss. Similarly, the destruction of a highly sensitive asset that doesn‘t play a critical role in productivity won‘t directly result in a significant productivity loss. Yet that same asset, if disclosed, can result in significant loss of competitive advantage or reputation, and generate legal costs. The point is that it‘s the combination of the asset and type of action against the asset that determines the fundamental nature and degree of loss. Which action(s) a threat agent takes will be driven primarily by that agent‘s motive (e.g., financial gain, revenge, recreation, etc.) and the nature of the asset. For example, a threat agent bent on financial gain is less likely to destroy a critical server than they are to steal an easily pawned asset like a laptop.

It is important to separate the concept of the event that a threat agent get in contact with the asset (even virtually, i.e. through the network) and the event that a threat agent act against the asset.

The term *Threat Agent* is used to indicate an individual or group that can manifest a threat. It is fundamental to identify who would want to exploit the assets of a company, and how they might use them against the company.

Threat Agent = Capabilities + Intentions + Past Activities

These individuals and groups can be classified as follows:

- Non-Target Specific: Non-Target Specific Threat Agents are computer viruses, worms, Trojans and logic bombs.
- Employees: Staff, contractors, operational/maintenance personnel, or security guards who are annoyed with the company.
- Organized Crime and Criminals: Criminals target information that is of value to them, such as bank accounts, credit cards or intellectual property that can be converted into money. Criminals will often make use of insiders to help them.
- Corporations: Corporations are engaged in offensive information warfare or competitive intelligence. Partners and competitors come under this category.
- Human, Unintentional: Accidents, carelessness.
- Human, Intentional: Insider, outsider.
- Natural: Flood, fire, lightning, meteor, earthquakes.

www.masomomsingi.co.ke

- ***Sources of threats***

A threat sources are those who wish a compromise to occur. It is a term used to distinguish them from threat agents/actors who are those who actually carry out the attack and who may be commissioned or persuaded by the threat actor to knowingly or unknowingly carry out the attack.

Threat communities

The following threat communities are examples of the human malicious threat landscape many organizations face:

- Internal
  - Employees
  - Contractors (and vendors)
  - Partners
- External
  - Cyber-criminals (professional hackers)
  - Spies
  - Non-professional hackers
  - Activists
  - Nation-state intelligence services (e.g., counterparts to the CIA, etc.)
  - Malware (virus/worm/etc.) authors

Threat action

Threat action is an assault on system security.
Completesecurity architecture deals with both intentional acts (i.e. attacks) and accidental events.Various kinds of threat actions are defined as subentries under "threat consequence".

Threat analysis

Threat analysis is the analysis of the probability of occurrences and consequences of damaging actions to a system. It is the basis of risk analysis.

Threat consequenceis a security violation that results from a threat action.It includes disclosure, deception, disruption, and usurpation. The following subentries describe four kinds of threat consequences, and also list and describe the kinds of threat actions that cause each consequence. Threat actions that are accidental events are marked by "*".

1 **Unauthorized disclosure** (a threat consequence)

A circumstance or event whereby an entity gains access to data for which the entity is not authorized. (See: data confidentiality.). The following threat actions can cause unauthorized disclosure:
Exposure:A threat action whereby sensitive data is directly released to an unauthorized entity. This includes:
Deliberate Exposure: Intentional release of sensitive data to an unauthorized entity.

www.masomomsingi.co.ke

Scavenging:Searching through data residue in a system to gain unauthorized knowledge of sensitive data.

* Human error

Human action or inaction that unintentionally results in an entity gaining unauthorized knowledge of sensitive data

* Hardware/software error

System failure that results in an entity gaining unauthorized knowledge of sensitive data

Interception:A threat action whereby an unauthorized entity directly accesses sensitive data travelling between authorized sources and destinations. This includes:

Theft:Gaining access to sensitive data by stealing a shipment of a physical medium, such as a magnetic tape or disk, that holds the data.

Wiretapping (passive):Monitoring and recording data that is flowing between two points in a communication system (See: wiretapping.)

Emanations analysis

Gaining direct knowledge of communicated data by monitoring and resolving a signal that is emitted by a system and that contains the data but is not intended to communicate the data. (See: Emanation.)

Inference: A threat action whereby an unauthorized entity indirectly accesses sensitive data (but not necessarily the data contained in the communication) by reasoning from characteristics or byproducts of communications. This includes:

Traffic analysis:Gaining knowledge of data by observing the characteristics of communications that carry the data.

Signals analysis: Gaining indirect knowledge of communicated data by monitoring and analyzing a signal that is emitted by a system and that contains the data but is not intended to communicate the data. (See: Emanation.)

Intrusion:A threat action whereby an unauthorized entity gains access to sensitive data by circumventing a system's security protections. This includes:

Trespass: Gaining unauthorized physical access to sensitive data by circumventing a system's protections.

Penetration: Gaining unauthorized logical access to sensitive data by circumventing a system's protections.

Reverse engineering: Acquiring sensitive data by disassembling and analyzing the design of a system component

Cryptanalysis: Transforming encrypted data into plain text without having prior knowledge of encryption parameters or processes.

www.masomomsingi.co.ke

THIS IS A SAMPLE
COMPLETE NOTES ARE IN SOFT AND IN HARD COPY
CALL|TEXT|WHATSAPP 0728 776 317
OR
Email: info@masomomsingi.co.ke

TOPIC 3

SYSTEMS SECURITY

- ***Classification***

An important aspect of information security and risk management is recognizing the value of information and defining appropriate procedures and protection requirements for the information. Not all information is equal and so not all information requires the same degree of protection. This requires information to be assigned a security classification.

The first step in information classification is to identify a member of senior management as the owner of the particular information to be classified. Next, develop a classification policy. The policy should describe the different classification labels, define the criteria for information to be assigned a particular label, and list the required security controls for each classification.

Some factors that influence which classification information should be assigned include how much value that information has to the organization, how old the information is and whether or not the information has become obsolete. Laws and other regulatory requirements are also important considerations when classifying information.

The Business Model for Information Security enables security professionals to examine security from systems perspective, creating an environment where security can be managed holistically, allowing actual risks to be addressed.

The type of information security classification labels selected and used will depend on the nature of the organization, with examples being:

- In the business sector, labels such as: **Public, Sensitive, Private, and Confidential**.
- In the government sector, labels such as: **Unclassified**, **Unofficial**, **Protected**, **Confidential**, **Secret**, **Top Secret** and their non-English equivalents.
- □ In cross-sectorial formations, the Traffic Light Protocol, this consists of: White, Green, Amber, and Red.

www.masomomsingi.co.ke

THIS IS A SAMPLE
COMPLETE NOTES ARE IN SOFT AND IN HARD COPY
CALL|TEXT|WHATSAPP 0728 776 317
OR
Email: info@masomomsingi.co.ke

TOPIC 4

PHYSICAL AND LOGICAL SECURITY

- ***Physical security***

Physical security is the protection of personnel, hardware, programs, networks, and data from **physical** circumstances and events that could cause serious losses or damage to an enterprise, agency, or institution. This includes protection from fire, natural disasters, burglary, theft, vandalism, and terrorism

Physical security is often overlooked (and its importance underestimated) in favor of more technical and dramatic issues such as hacking, viruses, Trojans, and spyware. However, breaches of physical security can be carried out with little or no technical knowledge on the part of an attacker. Moreover, accidents and natural disasters are a part of everyday life, and in the long term, are inevitable.

There are three main components to physical security. First, obstacles can be placed in the way of potential attackers and sites can be hardened against accidents and environmental disasters. Such measures can include multiple locks, fencing, walls, fireproof safes, and water sprinklers. Second, surveillance and notification systems can be put in place, such as lighting, heat sensors, smoke detectors, intrusion detectors, alarms, and cameras. Third, methods can be implemented to apprehend attackers (preferably before any damage has been done) and to recover quickly from accidents, fires, or natural disasters.

- ***Logical security (authentication, access rights. Others)***

Logical Security consists of software safeguards for an organization‘s systems, including user identification and password access, authenticating, access rights and authority levels. These measures are to ensure that only authorized users are able to perform actions or access information in a network or a workstation. It is a subset of computer security.

www.masomomsingi.co.ke

THIS IS A SAMPLE
COMPLETE NOTES ARE IN SOFT AND IN HARD COPY
CALL|TEXT|WHATSAPP 0728 776 317
OR
Email: info@masomomsingi.co.ke

TOPIC 5

DATA/SOFTWARE SECURITY

- ***Use of the normal security systems***
- ***Vulnerability assessment***

Vulnerability analysis, also known as vulnerability assessment, is a process that defines, identifies, and classifies the security holes (vulnerabilities) in a computer, network, or communications infrastructure. In addition, vulnerability analysis can forecast the effectiveness of proposed countermeasures and evaluate their actual effectiveness after they are put into use

Vulnerability analysis consists of several steps:

- Defining and classifying network or system resources
- Assigning relative levels of importance to the resources
- Identifying potential threats to each resource
- Developing a strategy to deal with the most serious potential problems first
- Defining and implementing ways to minimize the consequences if an attack occurs.

If security holes are found as a result of vulnerability analysis, a vulnerability disclosure may be required. The person or organization that discovers the vulnerability, or a responsible industry body such as the Computer Emergency Readiness Team (CERT), may make the disclosure. If the vulnerability is not classified as a high level threat, the vendor may be given a certain amount of time to fix the problem before the vulnerability is disclosed publicly.

The third stage of vulnerability analysis (identifying potential threats) is sometimes performed by a white hat using ethical hacking techniques. Using this method to assess vulnerabilities, security experts deliberately probe a network or system to discover its weaknesses. This process provides guidelines for the development of countermeasures to prevent a genuine attack.

Vulnerabilities and attacks

Vulnerability is a system susceptibility or flaw, and much vulnerability are documented in the Common Vulnerabilities and Exposures (CVE) database and vulnerability management is the cyclical practice of identifying, classifying, remediating, and mitigating vulnerabilities as they are discovered. An *exploitable* vulnerability is one for which at least one working attack or "exploit" exists.

To secure a computer system, it is important to understand the attacks that can be made against it, and these threats can typically be classified into one of the categories below:

www.masomomsingi.co.ke

Backdoors

A backdoor in a computer system, a cryptosystem or an algorithm, is any secret method of bypassing normal authentication or security controls. They may exist for a number of reasons, including by original design or from poor configuration. They may also have been added later by an authorized party to allow some legitimate access or by an attacker for malicious reasons; but regardless of the motives for their existence, they create vulnerability.

Denial-of-service attack

Denial of service attacks are designed to make a machine or network resource unavailable to its intended users. Attackers can deny service to individual victims, such as by deliberately entering a wrong password enough consecutive times to cause the victim account to be locked, or they may overload the capabilities of a machine or network and block all users at once. While a network attack from a single IP address can be blocked by adding a new firewall rule, many forms of Distributed denial of service (DDoS) attacks are possible, where the attack comes from a large number of points - and defending is much more difficult. Such attacks can originate from the zombie computers of a botnet, but a range of other techniques are possible including reflection and amplification attacks, where innocent systems are fooled into sending traffic to the victim.

Direct-access attacks

Common consumer devices that can be used to transfer data surreptitiously

An unauthorized user gaining physical access to a computer is often able to directly download data from it. They may also compromise security by making operating system modifications, installing software worms, keyloggers, or covert listening devices. Even when the system is protected by standard security measures, these may be able to be by passed by booting another operating system or tool from a CD-ROM or other bootable media. Disk encryption and Trusted Platform Module are designed to prevent these attacks.

Eavesdropping

Eavesdropping is the act of surreptitiously listening to a private conversation, typically between hosts on a network. For instance, programs such as Carnivore and NarusInsight have been used by the FBI and NSA to eavesdrop on the systems of internet service providers. Even machines that operate as a closed system (i.e., with no contact to the outside world) can be eavesdropped upon via monitoring the faint electro-magnetic transmissions generated by the hardware; TEMPEST is a specification by the NSA referring to these attacks.

Spoofing

Spoofing of user identity describes a situation in which one person or program successfully masquerades as another by falsifying data.

www.masomomsingi.co.ke

Tampering

Tampering describes a malicious modification of products. So-called "Evil Maid" attacks and security services planting of surveillance capability into routers are examples.

Privilege escalation

Privilege escalation describes a situation where an attacker with some level of restricted access is able to, without authorization, elevate their privileges or access level. So for example a standard computer user may be able to fool the system into giving them access to restricted data; or even to "become root" and have full unrestricted access to a system.

Phishing

Phishing is the attempt to acquire sensitive information such as usernames, passwords, and credit card details. Phishing is typically carried out by email spoofing or instant messaging, and it often directs users to enter details at a fake website whose look and feel are almost identical to the legitimate one.

Clickjacking

Clickjacking, also known as "UI redress attack or User Interface redress attack", is a malicious technique in which an attacker tricks a user into clicking on a button or link on another webpage while the user intended to click on the top level page. This is done using multiple transparent or opaque layers. The attacker is basically "hijacking" the clicks meant for the top level page and routing them to some other irrelevant page, most likely owned by someone else. A similar technique can be used to hijack keystrokes. Carefully drafting a combination of style sheets, iframes, buttons and text boxes, a user can be led into believing that they are typing the password or other information on some authentic webpage while it is being channeled into an invisible frame controlled by the attacker.

Social engineering and Trojans

Social engineering aims to convince a user to disclose secrets such as passwords, card numbers, etc. by, for example, impersonating a bank, a contractor, or a customer.

www.masomomsingi.co.ke

THIS IS A SAMPLE
COMPLETE NOTES ARE IN SOFT AND IN HARD COPY
CALL|TEXT|WHATSAPP 0728 776 317
OR
Email: info@masomomsingi.co.ke

TOPIC 6

TRANSMISSION SECURITY

Definition -Transmission Security (TRANSEC)

Transmission security (TRANSEC) is the process of securing data transmissions from being infiltrated, exploited or intercepted by an individual, application or device. TRANSEC secures data as it travels over a communication medium. It is generally implemented in military and government organization networks and devices, such as radar and radio communication equipment.

Transmission Security (TRANSEC) explained

TRANSEC is part of communication security (COMSEC) and is implemented and managed through several techniques, such as burst encoding, spread spectrum and frequency hopping. Each transmission stream is secured through a transmission security key (TSK) and cryptographic algorithm. Both the TSK and algorithm enable the creation of a pseudorandom sequence on top of the transmitted data. The key goals and objectives of TRANSEC are:

- To create a low probability of interception (LPI) for transmissions
- To create a low probability of detection (LPD) for the measures TRANSEC takes
- To ensure anti-jam, or resistance to jamming

Security: Secure Internet Data Transmission.

Sniff, spoof, encryption

- □ What Is Transmission Security?
- □ How Information Is Transmitted
- □ How Information Is Intercepted and Read
- □ Sniffing Devices
- □ Devices for Spoofing
- □ Methods of Transmissions and Their Levels of Security
- □ Encryption
  - o Why Use Encryption?
  - o Private Key Encryption
  - o Public Key Encryption
  - o State-of-the-Art Encryption and Its Future
- □ Why a Technical Solution Is Never the Whole Solution
- □ Client/Server Issues
- □ Secure Computing in Practice
  - o File Transmission
  - o Interactive Transmission

www.masomonsingi.co.ke

- How Much Is Too Much?
- What Level of Security Is Right for You?
- Summary

In the two preceding chapters we examined ways in which to keep your data safe, mainly from within an organization. I discussed the best ways to keep hackers out of your intranet and how to protect actual data from viruses and human error as well as the physical security of your software and hardware. Now that you've secured your tools and applications physically and have taken all precautions internally to keep data safe, it's time to consider how safe your data is during transmission. This transmission from one computer to another could be within your LAN, within your intranet, or over the Internet.

This chapter's topic, secure transmission, explores the security risks involved with data transmission, such as eavesdropping and decrypting. It discusses why and how to establish secure channels as well as ways to prevent or foil attacks on these secure channels. It's aimed primarily at anyone who is trying to design a fully secure system of computers and data or for anyone interested in encrypting data for transmission. Any individual involved with transmitting sensitive data-whether in a business that exchanges confidential information, either inside its corporate headquarters or with customers, or in an organization that exchanges any sensitive data between just two computers-should not skip this chapter. This includes banks; corporations with offices in different geographical locations that share proprietary information, regardless of whether it's public or private; or individuals doing business on the Internet, including selling products and conducting business transactions.

What Is Transmission Security?

Transmission security is the capability to send a message electronically from one computer system to another computer system so that only the intended recipient receives and reads the message and the message received is identical to the message sent. The message would not be identical if it was altered in anyway, whether transmitted over faulty channels or intercepted by an eavesdropper. Transmission security translates into secure networks. Although many people regard networks as computers connected by wires, this definition of a network, while technically correct, misses the point. Rather, networks are transmitted data, the data flowing over wires.

All transmissions can be intercepted. And the cautious user looks at all transmissions as if they will be intercepted. You can minimize the risks of transmission interception, but you can never, under any circumstances, completely rule it out. After all, it is people who design and put wires in their place, and people can get to them. Accessing wires is somewhat comparable, although much more difficult, to accessing a transmission sent over airwaves, as on a CB radio. For example, as a ham, you may have a message intended only for other hams. Although hams are the main communicators on these frequencies, anyone with the right radio equipment can tune in and listen, so it's likely your message will be received and heard by other listeners who pick up the frequency, whether you want them to hear it or not.

Similar risks occur with cellular phones, even though most transmission takes place over wire and not air. One risky transmission occurred between Prince Charles and his mistress Camilla

www.masomomsingi.co.ke

Parker Bowles when an eavesdropper intercepted a now infamous cellular phone conversation between the two.

How Information Is Transmitted

Most networking schemes involve data transmission over certain whole sections of the network. Most network transmissions don't go directly from computer A to computer B. Ethernet networks; for example, involve transmission to all directly connected computers on the local network. Two computers are "directly connected" if there is no device between them that filters the transmission based on its destination. So if computer A sends a message to computer E, computers B, C, and D will receive the message but will ignore it, because it is not intended for them, as shown in Figure 16.1. Many other types of networks, including Token Ring, FDDI, and some switched Ethernets operate on the same idea: Transmitted packets go to many devices on the network and expect the recipients to ignore messages destined for other computers. This is much like radio or television transmission, in which signals are sent out in every direction, but radios and TVs not on the correct station don't use the signal.

How Information Is Intercepted and Read

Any computer with access to the physical network wire or in the vicinity of over-air transmissions, however, could be instructed not to ignore the signals intended for other computers. This is the essence of electronic eavesdropping.

Information is considered intercepted when someone other than the intended recipient receives the information. Data can be intercepted in many ways, such as electronic eavesdropping or by using the recipient's password. It can occur anywhere, including in a chat room or through an e-mail exchange.

The tools required to read the transmission depend on how the information is intercepted. If an intruder is stealing transmissions at the most basic level (stealing the data packets straight off the wire or out of the air), the interloper will need something that translates electronic signals from voltage changes to the numbers and letters that those changes represent. Computers for which the transmission is intended do this automatically, because they are expecting the signal and already know its characteristics, how to decode it, and what to do with it. A much simpler method would be intercepting a message by just looking over someone's shoulder to read what they have written. Again, the legitimate user already has a context in which to interpret the on-screen information. The snooper, however, still has to interpret the message, and this isn't always so simple.

Sniffing Devices

There are troubleshooting programs and devices designed to analyze LAN traffic. These are commonly referred to as *packet sniffers,* because they are created to "sniff" packets of data for the network engineer. As mentioned in the preceding section, all transmissions are broadcast over all the wires. When one computer wants to communicate with another, it sends out an electrical signal through the network, which could be copper wire, fiber optic cable, or air. The

www.masomomsingi.co.ke

signal travels over this whole section of the network until it reaches the end of its signal strength in the air, the end of the wire or cable, or a network device that turns the packet back because the packet's destination is not on the other side of the device. At each point along this journey that the signal encounters a network interfaces, that interface examines the signal. If the interface sees the signal is for someone else, it ignores it. If the interface recognizes a signal for it, it reads it and gives it to the other parts of the computer for interpretation and use.

The nice thing about LANs is that the systems administrator can use a sniffer to tap into the wire to examine it. A systems administrator should occasionally examine these lines to check on the raw material going over the LAN. This is where packet sniffers are helpful. Packet sniffers will instruct your computer to look at every signal over the wire or only signals that meet certain criteria. This allows the systems administrator to analyze and actually read electrical signals. However, anyone with malicious intent also can use packet sniffers for analyzing and reading network traffic.

Now, you might think there are users out there maliciously using packet sniffers to read data worldwide, continuously. It's true that there may be many users with malicious intent snooping around networks, but it is not as simple as just purchasing a packet sniffer. There are devices-generally referred to as *internetworking devices* and more specifically referred to as *routers* and *bridges*-that actually filter the electrical signals sent out as data packets. These devices filter signals logically, which means that any data passing through a bridge or router must be intended to go through that bridge or router; the destination of the data must be on the other side of the internetworking device to get through the filter. If the destination of the data is not on the other side of the filter, the internetworking device won't pass the signal; and if it doesn't pass the signal, someone on the other side is unable to sniff the information, as shown in Figure 16.2. Anytime you have a network that requires any sort of logical divisions, you need an internetworking device. If you are connected to the Internet, you have an internetworking device. If your local network spans a large physical distance, you have some sort of internetworking device.

Figure 16.2: *This sniffer cannot smell packets on the other side of the router*.

Devices for Spoofing

Spoofing is somewhat of an overrated threat. *Spoofing* means getting your computer to pretend it is a different computer. The user forces the computer to present credentials to the network that are false. To do so, the user doesn't need tools but rather information to make those credentials realistic. The Internet identifies computers by numbers: Every computer has a unique number on the Internet.

www.masomomsingi.co.ke

THIS IS A SAMPLE
COMPLETE NOTES ARE IN SOFT AND IN HARD COPY
CALL|TEXT|WHATSAPP 0728 776 317
OR
Email: info@masomomsingi.co.ke

TOPIC 7

ICT RISK MANAGEMENT

IT risk management is the application of risk management methods to Information technology in order to manage IT risk, i.e.: The business risk associated with the use, ownership, operation, involvement, influence and adoption of IT within an enterprise or organization
IT risk management can be considered a component of a wider enterprise risk management system.

The establishment, maintenance and continuous update of an ISMS provide a strong indication that a company is using a systematic approach for the identification, assessment and management of information security risks.
Different methodologies have been proposed to manage IT risks, each of them divided in processes and steps.

According to Risk IT, it encompasses not just only the negative impact of operations and service delivery which can bring destruction or reduction of the value of the organization, but also the benefit\value enabling risk associated to missing opportunities to use technology to enable or enhance business or the IT project management for aspects like overspending or late delivery with adverse business impact.

Because risk is strictly tied to uncertainty, Decision theory should be applied to manage risk as a science, i.e. rationally making choices under uncertainty.
Generally speaking, risk is the product of likelihood times impact (Risk = Likelihood * Impact). The measure of an IT risk can be determined as a product of threat, vulnerability and asset values:

Risk = Threat * Vulnerability * Asset

A more current Risk management framework for IT Risk would be the TIK framework: Risk = ((Vulnerability * Threat) / Counter Measure) * Asset Value at Risk IT Risk.

Definitions

"Risk management is the process of identifying vulnerabilities and threats to the information resources used by an organization in achieving business objectives, and deciding what countermeasures, if any, to take in reducing risk to an acceptable level, based on the value of the information resource to the organization."

There are two things in this definition that may need some clarification. First, the *process* of risk management is an ongoing iterative process. It must be repeated indefinitely. The business environment is constantly changing and new threats and vulnerability emerge every day. Second, the choice of countermeasures (controls) used to manage risks must strike a balance between productivity, cost, effectiveness of the countermeasure, and the value of the informational asset being protected.

www.masomomsingi.co.ke

Risk management is the process that allows IT managers to balance the operational and economic costs of protective measures and achieve gains in mission capability by protecting the IT systems and data that support their organizations' missions. This process is not unique to the IT environment; indeed it pervades decision-making in all areas of our daily lives.

The head of an organizational unit must ensure that the organization has the capabilities needed to accomplish its mission. These mission owners must determine the security capabilities that their IT systems must have to provide the desired level of mission support in the face of real world threats. Most organizations have tight budgets for IT security; therefore, IT security spending must be reviewed as thoroughly as other management decisions. A well-structured risk management methodology, when used effectively, can help management identify appropriate controls for providing the mission-essential security capabilities.

Risk management in the IT world is quite a complex, multi faced activity, with a lot of relations with other complex activities. The picture show the relationships between different related terms.

The American National Information Assurance Training and Education Center defines risk in the IT field as:

1. *The total process to identify, controls, and minimize the impact of uncertain events. The objective of the risk management program is to reduce risk and obtain and maintain DAA approval. The process facilitates the management of security risks by each level of management throughout the system life cycle. The approval process consists of three elements: risk analysis, certification, and approval.*
2. *An element of managerial science concerned with the identification, measurement, control, and minimization of uncertain events. An effective risk management program encompasses the following four phases:*
    1. A*Risk assessment, as derived from an evaluation of threats and vulnerabilities.*
    2. *Management decision.*
    3. *Control implementation.*
    4. *Effectiveness review.*
3. *The total process of identifying, measuring, and minimizing uncertain events affecting AIS resources. It includes risk analysis, cost benefit analysis, safeguard selection, security test and evaluation, safeguard implementation, and systems review.*
4. *The total process of identifying, controlling, and eliminating or minimizing uncertain events that may affect system resources. lt includes risk analysis, cost benefit analysis, selection, implementation and test, security evaluation of safeguards, and overall security review.*

Risk management as part of enterprise risk management

Some organizations have, and many others should have, a comprehensive Enterprise risk management (ERM) in place. The four objectives categories addressed, according to Committee of Sponsoring Organizations of the Treadway Commission (COSO) are:

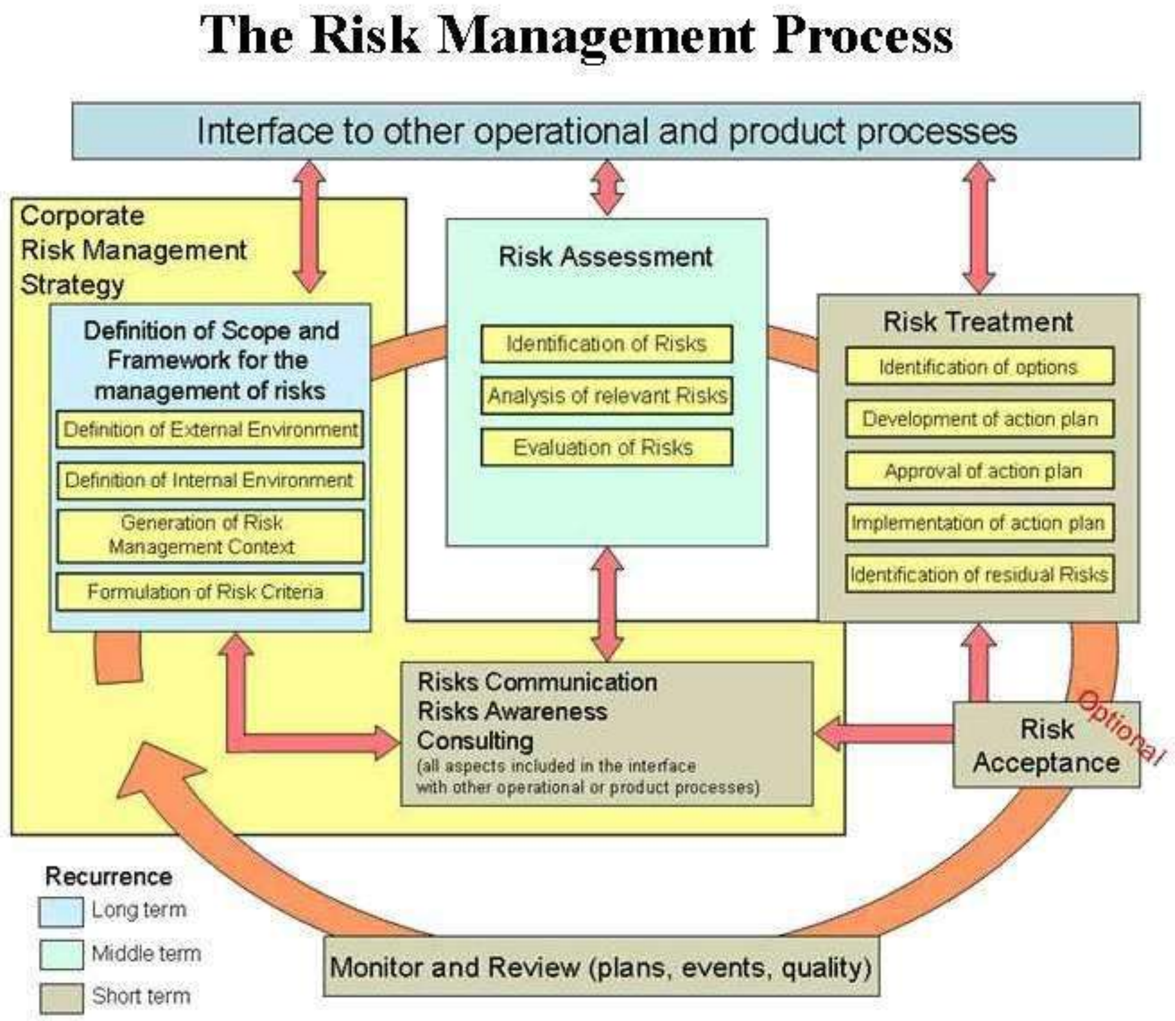
- Strategy - high-level goals, aligned with and supporting the organization's mission

www.masomomsingi.co.ke

- Operations - effective and efficient use of resources
- Financial Reporting - reliability of operational and financial reporting
- Compliance - compliance with applicable laws and regulations

According to Risk It framework by ISACA, IT risk is transversal to all four categories. The IT risk should be managed in the framework of Enterprise risk management: Risk appetite and Risk sensitivity of the whole enterprise should guide the IT risk management process. ERM should provide the context and business objectives to IT risk management

Risk management methodology


The Risk Management Process
Interface to other operational and product processes
Corporate Risk Management Strategy
Definition of Scope and Framework for the management of risks
Definition of External Environment
Definition of Internal Environment
Generation of Risk Management Context
Formulation of Risk Criteria
Risk Assessment
Identification of Risks
Analysis of relevant Risks
Evaluation of Risks
Risk Treatment
Identification of options
Development of action plan
Approval of action plan
Implementation of action plan
Identification of residual Risks
Risks Communication
Risks Awareness
Consulting
(all aspects included in the interface with other operational or product processes)
Risk Acceptance
Optional
Recurrence
Long term
Middle term
Short term
Monitor and Review (plans, events, quality)

ENISA: The Risk Management Process, according to ISO Standard 13335

The term methodology means an organized set of principles and rules that drive action in a particular field of knowledge. A methodology does not describe specific methods; nevertheless it does specify several processes that need to be followed. These processes constitute a generic framework. They may be broken down in sub-processes, they may be combined, or their sequence may change. However, any risk management exercise must carry out these processes in one form or another.

Due to the probabilistic nature and the need of cost benefit analysis, the IT risks are managed following a process that accordingly to NIST SP 800-30 can be divided in the following steps:

1. risk assessment,
2. risk mitigation, and
3. Evaluation and assessment.

Effective risk management must be totally integrated into the Systems Development Life Cycle.

Information risk analysis conducted on applications, computer installations, networks and systems under development should be undertaken using structured methodologies.

Context establishment

This step is the first step in ISOISO/IEC 27005 framework. Most of the elementary activities are foreseen as the first sub process of Risk assessment according to NIST SP 800-30. This step implies the acquisition of all relevant information about the organization and the determination of the basic criteria, purpose, scope and boundaries of risk management activities and the organization in charge of risk management activities. The purpose is usually the compliance with legal requirements and provide evidence of due diligence supporting an ISMS that can be certified. The scope can be an incident reporting plan, a business continuity plan.

Another area of application can be the certification of a product.

Criteria include the risk evaluation, risk acceptance and impact evaluation criteria. These are conditioned by:

- legal and regulatory requirements
- the strategic value for the business of information processes
- □ stakeholder expectations
- negative consequences for the reputation of the organization

Establishing the scope and boundaries, the organization should be studied: its mission, its values, its structure; its strategy, its locations and cultural environment. The constraints (budgetary, cultural, political, and technical) of the organization are to be collected and documented as guide for next steps.

Organization for security management

The setup of the organization in charge of risk management is foreseen as partially fulfilling the requirement to provide the resources needed to establish, implement, operate, monitor, review, maintain and improve an ISMS. The main roles inside this organization are:

www.masomomsingi.co.ke

- Senior Management

□ Chief information officer (CIO)

- System and Information owners
- the business and functional managers

□ the Information System Security Officer (ISSO) or Chief information security officer (CISO)

- IT Security Practitioners
- Security Awareness Trainers

- ***Risk management concepts***

Basic concepts

Risks exist because entities, companies and organisations have —assets‖ of a material or immaterial nature that could be subject to damage that has consequences on the entity in question.

Four concepts are important here:

• Assets, a term often used in the field of IT security
• Asset damage,
• Consequences for the entity,
• Possible but uncertain causes.

1. **Assets**

In very general terms, an asset can be defined as anything that could be of value or importance to the entity.

In information security, the ISO/IEC 27005 standarddistinguishes between

•Primary assets including

- Processes and activities,
- Information

•Supporting assets including:

- Equipment,
- Software,
- Networks,
- Personnel,
- Premises,
- Organisational support

www.masomomsingi.co.ke

THIS IS A SAMPLE
COMPLETE NOTES ARE IN SOFT AND IN HARD COPY
CALL|TEXT|WHATSAPP 0728 776 317
OR
Email: info@masomomsingi.co.ke

TOPIC 8

BUSINESS CONTINUITY PLANNING (BCP)

Business continuity planning (or **business continuity and resiliency planning**) is the process of creating systems of prevention and recovery to deal with potential threats to a company.
A business continuity plan is a plan to continue operations if a place of business is affected by different levels of disaster which can be localized short term disasters, to days long building wide problems, to a permanent loss of a building. Such a plan typically explains how the business would recover its operations or move operations to another location after damage by events like natural disasters, theft, or flooding. For example, if a fire destroys an office building or data center, the people and business or data center operations would relocate to a recovery site.
Any event that could negatively impact operations is included in the plan, such as supply chain interruption, loss of or damage to critical infrastructure (major machinery or computing /network resource). As such, risk management must be incorporated as part of BCP.In the US, government entities refer to the process as *continuity of operations planning* (COOP).

Analysis

The analysis phase consists of impact analysis, threat analysis and impact scenarios.

Business impact analysis (BIA)

A Business impact analysis (BIA) differentiates critical (urgent) and non-critical (non-urgent) organization functions/activities. Critical functions are those whose disruption is regarded as unacceptable. Perceptions of acceptability are affected by the cost of recovery solutions. A function may also be considered critical if dictated by law. For each critical (in scope) function, two values are then assigned:

- □ Recovery Point Objective (RPO) – the acceptable latency of data that will not be recovered. For example is it acceptable for the company to lose 2 days of data?
- □ Recovery Time Objective (RTO) – the acceptable amount of time to restore the function. The recovery point objective must ensure that the maximum tolerable data loss for each activity is not exceeded. The recovery time objective must ensure that the Maximum Tolerable Period of Disruption (MTPoD) for each activity is not exceeded.

Next, the impact analysis results in the recovery requirements for each critical function. Recovery requirements consist of the following information:

- The business requirements for recovery of the critical function, and/or
- The technical requirements for recovery of the critical function

THIS IS A SAMPLE
COMPLETE NOTES ARE IN SOFT AND IN HARD COPY
CALL|TEXT|WHATSAPP 0728 776 317
OR
Email: info@masomomsingi.co.ke

www.masomomsingi.co.ke

TOPIC 9

SYSTEM SECURITY POLICY IMPLEMENTATION

- ***Components of systems security policy***

Security Basics - Components of Security Policies
Policies are the heart of a security program. They are management's statement of support and expected outcomes from security controls. In this article, we examine the various components of a policy.

Components of a Security Policy

Policies form the basic framework of a security program. At the program level, policies represent senior management's security objectives. At the system level, they provide rules for the construction and operation of specific systems. Whether program or system specific, policies help prevent inconsistencies by forming the basis for detailed standards, guidelines, and procedures. They also serve as tools to inform employees about appropriate activities and restrictions required for regulatory compliance. Finally, policies make clear management's expectations of employee involvement in protecting information assets.

When building a policy, make sure it's clear and flexible. It shouldn't provide so much detail that it forces unreasonable constraints on operational areas of your business. Leave room to make management decisions that fit particular challenges as they arise.

Program policies establish the security program. They provide its form and character. The sections that make up a program policy include purpose, scope, responsibilities, and compliance. Following are the basic components of a security policy:

- **Purpose** includes the objectives of the program, such as:
  - Improved recovery times
  - Reduced costs or downtime due to loss of data
  - Reduction in errors for both system changes and operational activities
  - Regulatory compliance
  - Management of overall confidentiality, integrity, and availability
- **Scope** provides guidance on whom and what are covered by the policy. Coverage may include:
  - Facilities
  - Lines of business
  - Employees or departments
  - Technology
  - Processes
- **Responsibilities** for the implementation and management of the policy are assigned in this section. Organizational units or individuals are potential assignment candidates.

www.masomomsingi.co.ke

- **Compliance** provides for the policy's enforcement. Describe oversight activities and disciplinary considerations clearly. But the contents of this section are meaningless unless an effective awareness program is in place.

More note.

System specific policies provide the framework for system and issue specific security programs. Like program policies, system policies should be flexible enough to allow managers to make effective operational decisions while safeguarding the confidentiality, integrity, and availability of information assets. System policies typically address two areas: **security objectives and operational security standards.**

Policies that describe security objectives clearly define **measurable, achievable goals**. These goals focus on data owner directives intended to protect specific systems. The policies are written to take into account the system's functional requirements as seen by business users. Because policies apply constraints on how a system or a technology may be deployed and used, there's always a danger that meeting security objectives may adversely impact operational efficiency. It's important to balance reduction in risk with the cost associated with potential losses in productivity.

Operational security standards provide a clear set of rules for operating and managing a system or a technology. As with system policy objectives, these rules shouldn't be so restrictive that they paralyze your organization. In addition, the administrative burden associated with managing and enforcing overly restrictive policies may cost your organization more than the business impact you're trying to protect against. The elements of a system/issue specific policy include purpose, objectives, scope, roles and responsibilities, compliance, and policy owner and contact information.

- **Purpose** defines the challenge management is addressing. Challenges might include regulatory constraints, protection of highly sensitive data, or the safe use of certain technologies. In some cases, it may be necessary to define terms. It's important that everyone affected by the policy clearly understands its content. Finally, clearly state the conditions under which the policy is applicable.
- **Objectives** may include actions and configurations prohibited or controlled. Although they're normally defined outside a policy, circumstances and organizational practices may require placing certain standards and guidelines in this section. In any case, it's in this section that you define the results you expect from policy enforcement.
- **Scope** specifies where, when, how, and to whom the policy applies.
- **Roles and Responsibilities** identify the business units or individuals responsible for the various areas of implementation and enforcement of the policy.
- **Compliance** is just as important in a system or issue level policy as it is in a program policy. You should clearly state the possible consequences of not conforming to the standards and guidelines listed in Objectives.
- **Policy Owner and Contact Information** lists the person who is ultimately responsible for managing the policy. Since the data owner is responsible for defining the protection required for a specific system, she may be a good choice for policy owner. Ensure that contact information for the policy owner is kept up to date. This allows individuals responsible for implementing systems under the policy to contact the policy owner for clarification on standards and guidelines.

www.masomomsingi.co.ke

The final step in the construction of a policy is approval by senior management. Without their approval and support, a policy isn't worth very much. One way to ensure management support is to involve relevant areas of the business in the construction of each policy. This helps prevent the perception that information security policies, and information security in general, are an IS problem. It also nurtures a feeling of ownership across the organization. Managers are more willing to support operational restrictions that result in clear business value they helped define.

Although you can start with a blank sheet, I recommend you look at some example policies. A good place to start is the SANS Security Policy Project page .

- **Policy Implementation**
  After gaining management support and sign off, implementation planning begins. The roll out of a new policy includes the following activities:

1. Ensure everyone is aware of the new policy. Post it on your Intranet, send notification email, or perform whatever other mass distribution actions work well within your organization.
2. Discuss the content of the policy at management and staff meetings. It's important during these discussions to include a review of the intended results of following the policy. This helps your organization's employees see the standards and guidelines from the proper perspective.
3. Conduct training sessions. Training should occur at three levels - management, general staff, and technical staff.
   - Management training is intended to educate managers about their role in enforcement and compliance activities. It should include a "big picture" view of where the policy fits in the overall security program.
   - General staff training is provided to all staff levels in the organization. In addition to making employees aware of the contents of the policy, it should also address any questions about how the objectives, standards, and guidelines will impact day to day operation of the business. Staff training should always precede any attempts to sanction an employee for failure to follow a security policy.
   - Technical staff training is typically provided for the IS staff. The focus of this training is how the new policy affects existing system or network configurations and baselines.
4. Development of supporting standards, guidelines, procedures and baselines
5. Implement a user awareness program

What are the Components of a Security Policy?
A key point to consider is to develop a security policy that is flexible and adaptable as technology changes. Additionally, a security policy should be a living document routinely updated as new technology and procedures are established to support the mission of the organization.

The components of a security policy will change by organization based on size, services offered, technology, and available revenue. Here are some of the typical elements included in a security policy.

Security Definition – All security policies should include a well-defined security vision for the organization. The security vision should be clear and concise and convey to the readers the intent of the policy. In example:

www.masomomsingi.co.ke

―This security policy is intended to ensure the confidently, integrity, and availability of data and resources through the use of effective and established IT security processes and procedures.‖ Further, the definition section should address why the security policy is being implemented and what the corresponding mission will entail. This is where you tie the policy to the mission and the business rules of the organization.

Enforcement – This section should clearly identify how the policy will beenforced and how security breaches and/or misconduct will be handled.
The Chief Information Officer (CIO) and the Information Systems Security Officer (ISSO) typically have the primary responsibility for implementing the policy and ensuring compliance. However, you should have a member of senior management, preferably the top official, implement and embrace the policy. This gives you the enforcement clout and much needed _buy-in‘.
This section may also include procedures for requesting short-term exceptions to the policy. All exceptions to the policy should be reviewed and approved, or denied, by the Security Officer. Senior management should not be given the flexibility to overrule decisions. Otherwise, your security program will be full of exceptions that will lend themselves toward failure.

User Access to Computer Resources - This section should identify the roles and responsibilities of users accessing resources on the organization‘s network. This should include information such as:

- Procedures for obtaining network access and resource level permission;
- Policies prohibiting personal use of organizational computer systems;Passwords;
- Procedures for using removal media devices;
- Procedures for identifying applicable e-mail standards of conduct;
- Specifications for both acceptable and prohibited Internet usage;
- Guidelines for applications;
- Restrictions on installing applications and hardware;
- Procedures for Remote Access;
- Guidelines for use of personal machines to access resources (remote access);
- Procedures for account termination;
- Procedures for routine auditing;
- Procedures for threat notification; and
- Security awareness training;

www.masomomsingi.co.ke

THIS IS A SAMPLE
COMPLETE NOTES ARE IN SOFT AND IN HARD COPY
CALL|TEXT|WHATSAPP 0728 776 317
OR
Email: info@masomomsingi.co.ke

TOPIC 10

INTRODUCTION TO COMPUTER FORENSICS

- ***Computer forensics concepts***

Concepts and Standards

Regardless of specific case, technology used, concept of computer forensics is constant. Forensics case work consists of five basic steps:

1. **Preparation** – first and one of the most important step is proper forensic case preparation this can include: understanding local law and legal issues (this can determine tools and procedures we can or cannot use), understanding of assignment (what we are asked to do), reconnaissance of amount and type of computers and operation systems we will have to deal with. Preparing our team, checking equipment and much more…
2. **Collection** – from technical point of view distinguish three types of digital evidence collection models: First is on site acquisition – in this type we are making binary copy of hard drives, and then leave original ones. Second is evidence collecting and taking it to the lab where one can make acquisition. Third is live forensic when one is collecting evidences from powered on computers.

www.masomomsingi.co.ke

THIS IS A SAMPLE
COMPLETE NOTES ARE IN SOFT AND IN HARD COPY
CALL|TEXT|WHATSAPP 0728 776 317
OR
Email: info@masomomsingi.co.ke

TOPIC 11

PROFESSIONAL VALUES AND ETHICS IN COMPUTING

- ***Intellectual property and fraud***

Controlling Fraud and Protecting Intellectual Property: Today's Challenge

Even though data privacy is high on the security agenda these days, security has other important goals including protecting corporate data and intellectual property (IP) as well as controlling fraud. The relative importance of this protection will always be driven by the likelihood of attack, coupled with the value of the information or product that is lost. Stakes are clearly highest for organizations performing transactions in untrusted locations and over the Internet, those whose competitive position is driven by the data they own, or manufacturers of high value products, particularly in outsourced facilities. Examples of fraud include:

Risks

- In less-trusted manufacturing environments, insiders can potentially access valuable intellectual property, and authorize production overruns to build counterfeits. From a security perspective, they can manipulate device identities and corrupt embedded firmware and product configurations to stage wide-ranging attacks.
- Attackers can modify electronic documents, instructions, transactions and records to affect supply chain processes, legal claims, or the outcomes of decisions unless rigorous integrity tests are put in place.
- Organizations that cannot adequately protect outsourced manufacturing operations or online services will not only suffer direct financial losses but will also limit their flexibility to manage their business efficiently, potentially damaging their competitive position.
- Fraud and theft not only damage customer perceptions and experiences, but it also runs the risk of attracting the attention of regulators and compromising commercial and legal agreements with third parties such as content owners.

Controlling Fraud and Protecting Intellectual Property: Thales e-Security Solutions

Products and services from Thales e-Security can help many different types of organizations reduce the risk of fraud and theft of intellectual property. Cryptography can play a vital role in ensuring the confidentiality of information, particularly as it is exposed in hostile environments, and can be used to verify the integrity and authenticity of almost any form of electronic document or message. In some cases cryptographic protection, particularly in the form of encryption, can be easily deployed in a completely transparent way. Network level encryption using the Datacryptor family of encryption platforms can be used to protect virtually any form of backbone network connection and is particularly valuable in protecting virtual private networks (VPNs) to remote manufacturing or logistics locations.

www.masomomsingi.co.ke

Other forms or protection, specifically those that introduce the use of digital identities and digital signatures, rely on public key operations and typically rely on an underlying public key infrastructure (PKI). In some cases commercial applications support PKI-based techniques as standard; whereas in-house applications may need to be modified to support this more sophisticated but more secure approach to security. In all cases the protection of keys within a PKI and its associated applications needs to be strongly enforced and tightly managed. In this context the nShield hardware security module (HSM) is a perfect fit and benefits from pre-qualified integration with a host of leading commercial applications.

Looking beyond even key management, organizations also need to protect the application processes that actually use those keys, for example to approve the issuance of an embedded digital ID for a manufactured device, approve the loading of secure firmware, signing of a transaction, or counting of a vote. In remote and often untrusted locations these processes can be made secure only through advanced levels of physical and logical security. The CodeSafe capability of nShield HSMs enables high-tech manufacturers and software providers to create tamper-resistant processes that protect their critical processes, business models, and intellectual property, reducing the risk of abuses and counterfeiting. With CodeSafe, organizations can secure sensitive processes (such as identity management or metering) behind a physically tamper-resistant barrier. As a result, manufacturers can be more confident in their ability to outsource securely, while software providers can maximize revenue by enforcing license agreements through secure metering capabilities.

Benefits:

- Encrypt information to ensure confidentiality as it flows over networks, as it is stored, and as it is used—either within the corporate datacenter or at remote locations.
- Digitally sign documents, transactions, and messages to create a mechanism that can easily validate their integrity and authenticity.
- Comply with regional digital signing laws through the use of security certified HSMs to establish legally sound documents.
- Efficiently generate cryptographic keys and digital credentials to support high volume production processes with high assurance credential management capabilities for secure device authentication.
- Create secure outsourcing environments by establishing tamper-resistant, trusted environments to protect critical application processes such as software loading, license provisioning, and identity management.
- Strengthen critical web infrastructure with leading-edge DNS security capabilities (DNSSEC) to reduce the risk of web site spoofing and service disruption.

1. Criminal offences (counterfeiting and piracy)

Infringement of trademarks and copyrights can be criminal offences, as well as being actionable in civil law. A range of criminal provisions are set out in the relevant Acts, and other offences such as those under the Fraud Act 2006 may also be applied. These criminal offences are most often associated with organized crime groups who are dealing for profit in fake branded goods or pirated products. However, these offences can also occur in legitimate business, for example if

www.masomomsingi.co.ke

an employee uses the workplace to produce and/or sell quantities of fake DVDs or branded goods to colleagues or outside the office.

1.1. What is criminal intellectual property (IP) rights infringement?

Criminal IP offences are also known as ―IP crime‖ or ―counterfeiting‖ and ―piracy‖. Counterfeiting can be defined as the manufacture, importation, distribution and sale of products which falsely carry the trade mark of a genuine brand without permission and for gain or loss to another. Piracy, which includes copying, distribution, importation etc. of infringing works, does not always require direct profits from sales - wider and indirect benefits may be enough along with inflicting financial loss onto the rights holder. For example possession of an infringing copy of a work protected by copyright in the course of your business may be a criminal offence under section 107 (1)(c) of the Copyright, Designs and Patents Act 1988.

Not all cases that fall within the criminal law provisions will be dealt with as criminal offences and in many cases business to business type disputes are tackled by the civil law. Further information is available on what is the law and the guide to offences.

1.2. What does infringement mean

―Infringement‖ is a legal term for an act that means breaking a law. IP rights are infringed when a product, creation or invention protected by IP laws are exploited, copied or otherwise used without having the proper authorization, permission or allowance from the person who owns those rights or their representative.

It can range from using technology protected by a patent to selling counterfeit medicines/software or copying a film and making it available online.

All of these acts will constitute a civil infringement but some copyright and trade mark infringements may also be a criminal offence such as the sale of counterfeits including clothing.

1.3. How will action be taken against you

Trading standards are primarily responsible for enforcing the criminal IP laws, with support from the police, and with investigative assistance from the IP rights owners. Private criminal investigations and prosecutions may also be launched by the right owners in some cases.

Criminal IP offences may be taking place in your workplace in a variety of ways. These include:

- employees selling copies of protected works or supplying fake goods within the working environment
- company servers and equipment being used to make available (i.e. uploading) infringing content to the internet with the knowledge of management
- using the work intranet to offer for sale infringing products to colleagues
- external visitors entering your premises, to sell counterfeit and pirated items

www.masomonsingi.co.ke

- using unlicensed software on business computer systems with the knowledge of management

Not only can IP crime make you and your business liable to a potential fine of up to £50,000, and a custodial sentence of up to 10 years, counterfeiting and piracy can affect your business security and reputation, threaten your IT infrastructure and risk the health and safety of your staff and consumers.

2 Risks for business

IP rights infringement and in particular IP crime threaten legitimate businesses, their staff, and undermines consumer confidence. Your business may face a number of risks if you do not take appropriate steps to tackle IP crime within your working environment.

Failure to address the problem could leave you and your business liable and at risk to criminal and/or civil action. Under civil law you may be subject to court action and have to pay damages. Criminal action may lead to unlimited fines, or a custodial sentence (which could be up to a maximum of 10 years). You may also be vulnerable to threats from computer viruses and malware.

You need to think about not only the way your business is conducted, but also be aware that the behaviour of your staff – and their actions at work may also incur liability for the organisation as a whole.

2.1. Legal liability

Activities which results in IP rights being infringed can raise both civil and criminal law liabilities. In some cases these activities may relate to something done directly by the business. In other instances it may relate to an independent action of a member of staff at work.

2.2. Security risks

www.masomomsingi.co.ke

THIS IS A SAMPLE
COMPLETE NOTES ARE IN SOFT AND IN HARD COPY
CALL|TEXT|WHATSAPP 0728 776 317
OR
Email: info@masomomsingi.co.ke

www.masomomsingi.co.ke