INFORMATION SYSTEM SECURITY AND AUDIT

The Guide provides Knowledge in the following Areas:

- **Information system Security, Control & Audit**
- **Continuity of Computer Operations**
- **Governance**

FOREWORD

Cybercrime appears unstoppable, there are thousands of cybercrimes every year, ranging in cost from a few hundred dollars to the millions. From the report compiled by Z. Smith et.al (2021), since 2018, it is estimated that the cost of global cybercrime reached over $1 trillion. The estimated the monetary loss from cybercrime was approximately $945 billion, this average cost rose steadily from $300 billion in 2013 to $475 billion in 2014 to $522 billion in 2018.

what accounts for this increase is that cybercriminals are using more effective techniques, with cybercriminals "actively targeting non-financial organizations that include healthcare bodies, pharmaceutical companies, academia, medical research organizations, and local governments; this is mind boggling in the first glowing IT sector.

The risk of cybercrime to operations and profits continues to grow for many organizations. Global spending on cyber security, was expected to exceed $145 billion in 2020.

In the research for smith report a total of 1,500 companies were surveyed, only 4% claimed that they did not experience any sort of cyber incident in 2019.The damage from malware and spyware represented the highest cost to organizations, closely followed by data breaches. Affected companies said the biggest non-monetary loss was in productivity and lost work hours.
Despite this, it was found that most organizations do not have plans in place to reduce the effect of security incidents on their operations. From the report slightly more than half of the surveyed organization said they do not have plans to both prevent and respond to a cyber-incident. Out of the 951 organizations that had a response plan, only 32% said the plan was actually effective.

While many cyber-attacks can be managed in house, major incidents often require contracting with outside consultants at high rates, forming a significant portion of the cost of a large-scale incident. From the report Only 213 out of 1,332 surveyed companies reported that they dealt with cyber incidents without third-party support. Typically, they relied on cyber security organizations or response teams to help with ***CONTAINMENT, RECOVERY AND REMEDIATION,*** in most of these cases, consultants were used to assist in *containment, recovery and remediation*.
Cyber-attacks range from minor attacks that are easily handled in house to major breaches that require a coordinated response involving leadership throughout the organization, lawyers, public relations specialists, and cyber experts, many of whom must be brought in as consultants.

On December 14, 2021, Google asked its 2.6 billion Chrome users to update the browser urgently to fix a "critical" bug that was being exploited by hackers.

As cyber-attacks have become more prevalent, so have the consultants who can help remediate a major attack or breach that would otherwise overwhelm a victim organization. Many consulting firms provide cyber services, these consultancies continue to expand to meet demand for their services, with the shortage of qualified experts driving daily rates per consultant into the thousands of dollars. Fees paid to consulting firms are likely to be a significant component of the overall cost of responding to a major incident, for example the U.K.'s National Health Service spent a total of £73 million on IT support in response to the WannaCry attack, much of which went to outside consultants.

From a report compiled by Communications Authority of Kenya, National Kenya Computer Incident Response Team/Coordination (KE-CIRT/CC), in period July - September 2021, the National KE-CIRT/CC detected 143,040,599 cyber threat events, which was a 268.883% increase from the

38,776,699 threat events detected in the previous period, April - June 2021. This increase in cyber threat events detected is attributed to the significant increase in targeted attacks at critical systems and services; increased activity by ransom ware groups; adoption of more sophisticated tools by cyber threat actors; increased targeted attacks at Internet of Things (IoT) devices; increased exploits of third-party mobile application vulnerabilities; increased targeted attacks at unsecured infrastructure; and increased adoption of botnet and Distributed Denial of Service (DDoS) attack techniques. This is illustrated in the table below.

	Threats Detected	April-June 2021	July – September 2021
1	Malware	23,053,190	70,501,144
2	DDOS/Botnet	11,272,402	49,816,062
3	Web Application Attacks	2,564,173	478,123
4	System Vulnerabilities	1,886,934	22,245,270
	Totals	38,776,699	143,040,599

While opening Cyber Security Strategy 2022 – 2026 workshop in Naivasha in june 2022, interior and National Government Coordination Cabinet Secretary (CS), Dr. Fred Matiang`i, called on all players in the cyber space to work together in securing the cyber space. The minister said most of the private and government businesses are now being transacted on the cyber space which predisposes these businesses to cybercrime. He said the increase in technology and growth of the same has soared transactions from 1.9trillion 10 years ago to over 6.8trillion in 2022, indicating an urgent need to protect this space.

He further observed that the *Huduma Namba program* that was challenged in court was actually meant to protect individual data by putting it in a central place instead of it being scattered all over the place which make such data unsecure.

Cybercriminals find Africa an attractive scene to stage the attacks because many firms have yet to invest adequately in anti-hacking measures. Various reports indicate that various African countries, Kenyan among them, have in the recent past witnessed a surge in cases of cyber attacks.

“It’s alarming to think that Kenyan businesses are dealing with almost 540 more weekly cyber-attacks than their peers across the globe,” Pankaj Bhula, Check Point’s Regional Director for Africa told Digital Business.“This signals an urgent need for Kenya’s businesses to take a proactive approach to cybersecurity solutions, while focusing on companywide education on security hygiene to keep users and the business safe online.

When a small business owner is faced with the responsibilities of production economics, financial reports and marketing all at the same time, cybersecurity can often appear complicated and, at times, unnecessary. However, this disregard for IT security is being exploited by cybercriminals.

Companies and agencies need to do more to prevent cyber incidents from occurring. And they also need to do more to speed up service restoration, address business disruptions, and repair damage to employee morale and customer trust.

Bernard Mokua
Lecturer in Information system security

Chapter One
INTRODUCTION TO INFORMATION SYSTEMS

System is a set of interacting or interdependent components forming an integrated whole or a set of elements (often called *'components')* and relationships which are different from relationships of the set or its elements to other elements or sets.

Data consists of the raw facts representing events occurring in the organization before they are organized into an understandable and useful form for humans.

Information is data that has been processed in such a way as to be meaningful to the person who receives it. It provides context for data and enables decision making processes.

Uses of Information

Businesses and other organizations need information for many purposes: we have summarized the five main uses in the table below.

- ***Planning***

To plan properly, a business needs to know what resources it has (e.g. cash, people, machinery and equipment, property, customers). At the planning stage, information is important as a key ingredient in decision-making.

- ***Recording***

Information about each transaction or event is needed. Just as importantly, information needs to be recorded so that the business can be properly managed.

- ***Controlling***

Once a business has produced its plan it needs to monitor progress against the plan - and control resources to do so. So information is needed to help identify whether things are going better or worse than expected, and to spot ways in which corrective action can be taken

- ***Measuring***

Performance must be measured for a business to be successful. Information is used as the main way of measuring performance. For example, this can be done by collecting and analysing information on sales, costs and profits

- ***Decision-making***

i. Strategic information**:** used to help plan the objectives of the business as a whole and to measure how well those objectives are being achieved. Examples of strategic information include:
- Profitability of each part of the business
- Size, growth and competitive structure of the markets in which a business operates

ii.Tactical Information: this is used to decide how the resources of the business should be employed. Examples include:
- Information about business productivity (e.g. units produced per employee; staff turnover)

iii. Operational: Information: this information is used to make sure that specific operational tasks are carried out as planned/intended (i.e. things are done properly).

For example, a production manager will want information about the extent and results of quality control checks that are being carried out in the manufacturing process.

An Information System (IS) can be any organized combination of people, hardware, software, communications networks, data resources, and policies and procedures that stores, retrieves, transforms, and disseminates information in an organization.

*An important factor of computer based information system is **precision,** which may not apply to other types of systems.*

Information system

An information system is a combination of software, hardware, and telecommunication networks to collect useful data, especially in an organisation. Many businesses use information technology to complete and manage their operations, interact with their consumers, and stay ahead of their competition

Components of information systems

An information system is described as having five components.

Computer hardware

This is the physical technology that works with information. Hardware can be as small as a smartphone that fits in a pocket or as large as a supercomputer that fills a building.

Computer software

Software can be divided into two types: system software and application software.

Telecommunications

This component connects the hardware together to form a network. Connections can be through wires, such as Ethernet cables or fibre optics, or wireless, such as through Wi-Fi.

Databases /Data

A database is a place where data is collected and from which it can be retrieved by querying it using one or more specific criteria. A data warehouse contains all of the data in whatever form that an organization needs.

Human resources and procedures

the people that are needed to run the system and the procedures they follow so that the knowledge in the huge databases and data warehouses can be turned into learning that can interpret what has happened in the past and guide future action.

Computer security

Computer security basically is the protection of computer systems and information from harm, theft, and unauthorized use. It is the process of preventing and detecting unauthorized use of your computer system.

Computer security threats

Computer security threats are possible dangers that can possibly hamper the normal functioning of your computer. In the present age, cyber threats are constantly increasing as the world is going digital. The most harmful types of computer security are:

- Viruses

A computer virus is a malicious program which is loaded into the user's computer without user's knowledge. It replicates itself and infects the files and programs on the user's PC. The ultimate goal of a virus is to ensure that the victim's computer will never be able to operate properly or even at all.

- Computer Worm

A computer worm is a software program that can copy itself from one computer to another, without human interaction. The potential risk here is that it will use up your computer hard disk space because a worm can replicate in greate volume and with great speed.

- Phishing

Disguising as a trustworthy person or business, phishers attempt to steal sensitive financial or personal information through fraudulent email or instant messages. Phishing in unfortunately very easy to execute. You are deluded into thinking it's the legitimate mail and you may enter your personal information.

- Botnet

A botnet is a group of computers connected to the internet, that have been compromised by a hacker using a computer virus. An individual computer is called 'zombie computer'. The result of this threat is the victim's computer, which is the bot will be used for malicious activities and for a larger scale attack like DDoS.

- Rootkit

A rootkit is a computer program designed to provide continued privileged access to a computer while actively hiding its presence. Once a rootkit has been installed, the controller of the rootkit will be able to remotely execute files and change system configurations on the host machine.

- Keylogger

Also known as a keystroke logger, keyloggers can track the real-time activity of a user on his computer. It keeps a record of all the keystrokes made by user keyboard. Keylogger is also a very powerful threat to steal people's login credential such as username and password.

Cyber space

A global domain within the information environment consisting of the interdependent network of information systems infrastructures including the Internet, telecommunications networks, computer systems, and embedded processors and controllers i.e. concept describing a widespread interconnected digital technology.

Cyberspace is an embodied switched network for moving information traffic further characterized by varying degrees of access, navigation, information- activity, augmentation (and trust), and these characteristics can be taken into account sufficiently for drawing legal conclusions.

The control of cyberspace is thus important not only because of the actions of individual participants but because the infrastructure of cyberspace is now fundamental to the functioning of national and international security systems, trade networks, emergency services, basic communications, and other public and private.

Securing Cyber Space

Increased connectivity of people and devices to the Internet and to each other has created an ever-expanding attack surface that extends throughout the world. As a result, cyberspace has become the most active threat domain in the world and the most dynamic threat to the Homeland.
The huge increase in the use of digital technologies throughout the COVID-19 pandemic has led to far greater numbers of connected devices, increasing the attack surface for cyber criminals.

cyber space security
Focus on protecting computers, networks, programs and data from unintended or unauthorized access, change or destruction.

Chapter Two
RISKS, THREATS AND VULNERABILITIES

All *risks, threats, and vulnerabilities* are measured for their potential capability to compromise one or all of the AIC principles

a) Vulnerability

It is a software, hardware, or procedural weakness that may provide an attacker the open door he is looking for to enter a computer or network and have unauthorized access to resources within the environment.

Vulnerability characterizes the absence or weakness of a safeguard that could be exploited.

E.g.: a service running on a server, unpatched applications or operating system software, unrestricted modem dial-in access, an open port on a firewall, lack of physical security etc.

An application vulnerability is a system flaw or weakness in an application that could be exploited to compromise the security of the application. These crimes target the confidentiality, integrity, or availability (known as the "CIA triad") of resources possessed by an application, its creators, and its users.

b) Threat

Is any potential danger to information or systems. A threat is a possibility that someone (person, s/w) would identify and exploit the vulnerability.

The entity that takes advantage of vulnerability is referred to as a threat agent. E.g.: A threat agent could be an intruder accessing the network through a port on the firewall

Information systems are frequently exposed to various types of threats which can cause different types of damages that might lead to significant financial losses. Information security damages can range from small losses to entire information system destruction. The effects of various threats vary considerably: some affect the confidentiality or integrity of **data** while others affect the **availability of a system.**

Currently, organizations are struggling to understand what the threats to their information assets are and how to obtain the necessary means to combat them which continues to pose a challenge. To improve our understanding of security threats, we propose a security threat classification model which allows us to study the threats class impact instead of a threat impact as a threat varies over time.

Examples of Access Control Threats

Denial of Service (DoS/DdoS)

A denial-of-service attack (DoS attack) or distributed denial-of-service attack (DDoS attack) is an attempt to make a computer resource unavailable to its intended users. Although the means to, motives for, and targets of a DoS attack may vary, it generally consists of the concerted, malevolent efforts of a person or persons to prevent an Internet site or service from functioning efficiently or at all, temporarily or indefinitely.

The purpose of DoS attacks is to force the targeted computer(s) to reset, or consume its resources so that it can no longer provide its intended service

Types of DoS Attacks

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

- Consumption of computational resources, such as bandwidth, disk space, or CPU time;
- Disruption of configuration information, such as routing information;
- Disruption of state information, such as unsolicited resetting of TCP sessions;
- Disruption of physical network components.
- Obstructing the communication media between the intended users and the victim so that they can no longer communicate adequately.

Countermeasures

Unfortunately, there are no effective ways to prevent being the victim of a DoS or DDoS attack, but there are steps you can take to reduce the likelihood that an attacker will use your computer to attack other computers:

- Install and maintain anti-virus software.
- Install a firewall, and configure it to restrict traffic coming into and leaving your computer.
- Follow good security practices for distributing your email address.
-

Buffer Overflows

A buffer overflow is an anomalous condition where a process attempts to store data beyond the boundaries of a fixed-length buffer. The result is that the extra data overwrites adjacent memory locations. The overwritten data may include other buffers, variables and program flow data and may cause a process to crash or produce incorrect results. They can be triggered by inputs specifically designed to execute malicious code or to make the program operate in an unintended way. As such, buffer overflows cause many software vulnerabilities and form the basis of many exploits.

Buffer Overflow Techniques

- *Stack Buffer Overflow*
  - A stack buffer overflow occurs when a program writes to a memory address on the program's call stack outside of the intended data structure; usually a fixed length buffer.
  - Stack buffer overflow bugs are caused when a program writes more data to a buffer located on the stack than there was actually allocated for that buffer. This almost always results in corruption of adjacent data on the stack, and in cases where the overflow was triggered by mistake, will often cause the program to crash or operate incorrectly.
  - A technically inclined and malicious user may exploit stack-based buffer overflows to manipulate the program

- *Heap Buffer Overflow*
  - A heap overflow is another type of buffer overflow that occurs in the heap data area. Memory on the heap is dynamically allocated by the application at run-time and typically contains program data.
  - Exploitation goes as follows: If an application copies data without first checking to see if it fits into the chunk (blocks of data in the heap), the attacker could supply the application with a piece of data that is too large, overwriting heap management information (metadata)

of the next chunk. This allows an attacker to overwrite an arbitrary memory location with four bytes of data. In most environments, this may allow the attacker control over the program execution.

Countermeasure

- Choice of programming language
- Use of safe libraries
- Stack-smashing protection which refers to various techniques for detecting buffer overflows on stack-allocated variables. The most common implementation being StackGuard, and SSP
- Executable space protection which is the marking of memory regions as non-executable, such that an attempt to execute machine code in these regions will cause an exception. It makes use of hardware features such as the NX bit (Non Execute bit).
- Address space layout randomization: A technique which involves arranging the positions of key data areas, usually including the base of the executable and position of libraries, heap, and stack, randomly in a process' address space.
- Deep packet inspection: It is a form of computer network packet filtering that examines the data and/or header part of a packet as it passes an inspection point, searching for non-protocol compliance, viruses, spam, intrusions or predefined criteria to decide if the packet can pass or if it needs to be routed to a different destination, or for the purpose of collecting statistical information. It also called Content Inspection or Content Processing.

Spoofing/Masquerading

A spoofing attack is a situation in which one person or program successfully masquerades as another by falsifying data and thereby gaining an illegitimate advantage.

Popular Spoofing Techniques

- *Man-in-the-middle attack (MITM):* An attack in which an attacker is able to read, insert and modify at will messages between two parties without either party knowing that the link between them has been compromised. The attacker must be able to observe and intercept messages going between the two victims
- *IP address Spoofing* : refers to the creation of IP packets with a forged (spoofed) source IP address with the purpose of concealing the identity of the sender or impersonating another computing system.
- *URL spoofing*: A Spoofed URL describes one website that poses as another
- *Phishing* :An attempt to criminally and fraudulently acquire sensitive information, such as usernames, passwords and credit card details, by masquerading as a trustworthy entity in an electronic communication.
- *Referrer spoofing*:It is the sending of incorrect referrer information along with an HTTP request, sometimes with the aim of gaining unauthorized access to a web site. It can also be used because of privacy concerns, as an alternative to sending no referrer at all.
- *Spoofing of file-sharing Networks*: Polluting the file-sharing networks where record labels share files that are mislabeled, distorted or empty to discourage downloading from these sources.
- *Caller ID spoofing* :This allows callers to lie about their identity, and present false names and numbers, which could of course be used as a tool to defraud or harass
- *E-mail address spoofing:*A technique commonly used for spam e-mail and phishing to hide the origin of an e-mail message by changing certain properties of the e-mail, such as the From, Return-Path and Reply-To fields.

- *Login spoofing* : A technique used to obtain a user's password. The user is presented with an ordinary looking login prompt for username and password, which is actually a malicious program, usually called a Trojan horse under the control of the attacker. When the username and password are entered, this information is logged or in some way passed along to the attacker, breaching security.

Countermeasures

- Be skeptical of e-mails indicating that you need to make changes to your accounts or warnings indicating that accounts will be terminated without you doing some type of activity online.
- Call the legitimate company to find out if this is a fraudulent message.
- Review the address bar to see if the domain name is correct.
- When submitting any type of financial information or credential data, an SSL connection should be set up, which is indicated in the address bar and a closed-padlock icon in the browser at the bottom-right corner.

Shoulder Surfing

- Shoulder surfing refers to using direct observation techniques, such as looking over someone's shoulder, to get information. Shoulder surfing is particularly effective in crowded places because it's relatively easy to observe someone as they:
  - Fill out a form
  - Enter their PIN at an automated teller machine or a POS Terminal
  - Use a calling card at a public pay phone
  - Enter passwords at a cybercafe, public and university libraries, or airport kiosks.
  - Enter a digit code for a rented locker in a public place such as a swimming pool or airport.
- Shoulder surfing is also be done at a distance using binoculars or other vision-enhancing devices. To prevent shoulder surfing, it is advised to shield paperwork or the keypad from view by using one's body or cupping one's hand.
- Recent automated teller machines now have a sophisticated display which discourages shoulder surfers. It grows darker beyond a certain viewing angle, and the only way to tell what is displayed on the screen is to stand directly in front of it.

Object Reuse

Object reuse issues pertain to reassigning to a subject media that previously contained one or more objects.

The sensitive information that may be left by a process should be securely cleared before allowing another process the opportunity to access the object. This ensures that information not intended for this individual or any other subject is not disclosed.

For media that holds confidential information, more extreme methods should be taken to ensure that the files are actually gone, not just their pointers.

Countermeasures

- Sensitive data should be classified by the data owners.

- How the data is stored and accessed should also be strictly controlled and audited by software controls.
- Before allowing one subject to use media that was previously used, the media should be erased or degaussed. If media holds sensitive information and cannot be purged, there should be steps on how to properly destroy it so that there is no way for others to obtain this information.

Data Remanence

Data remanence is the residual representation of data that has been in some way been nominally erased or removed. This residue may be due to data being left intact by a nominal delete operation, or through physical properties of the storage medium.

Data remanence may make inadvertent disclosure of sensitive information possible, should the storage media be released into an uncontrolled environment.

Countermeasures

- Methods to Countermeasure
  - Overwriting
    - A common method used to counter data remanence is to overwrite the storage medium with new data. This is often called a wiping or shredding a file or disk. The simplest overwrite technique writes the same data everywhere -- often just a pattern of all zeros. At a minimum, this will prevent the data from being retrieved simply by reading from the medium again, and thus is often used for clearing.
  - Degaussing
    - Degaussing is the removal or reduction of a magnetic field. Applied to magnetic media, degaussing may purge an entire media element quickly and effectively
    - Degaussing often renders hard disks inoperable, as it erases low-level formatting which is only done at the factory, during manufacture.
  - Encryption
    - Encrypting data before it is stored on the medium may mitigate concerns about data remanence.
    - Encryption may be done on a file-by-file basis, or on the whole disk.
  - Physical destruction
    - Physical destruction of the data storage medium is generally considered the most certain way to counter data remanence, although also at the highest cost.

Backdoor/Trapdoor

A backdoor is a malicious computer program or particular means that provide the attacker with unauthorized remote access to a compromised system exploiting vulnerabilities of installed software and bypassing normal authentication.

A backdoor works in background and hides from the user. It is very similar to a virus and therefore is quite difficult to detect and completely disable.

A backdoor is one of the most dangerous parasite types, as it allows a malicious person to perform any possible actions on a compromised computer. The attacker can use a backdoor to:

- spy on a user,
- manage files,
- install additional software or dangerous threats,
- control the entire system including any present applications or hardware devices,
- shutdown or reboot a computer or

- attack other hosts.

Countermeasure

- Powerful antivirus and anti-spyware products

Dictionary Attacks

Dictionary attacks are launched by programs which are fed with a lists (dictionaries) of commonly used words or combinations of characters, and then compares these values to capture passwords. Once the right combination of characters is identified, the attacker can use this password to authenticate herself as a legitimate user.
Sometimes the attacker can even capture the password file using this kind of activity.

Countermeasures

To properly protect an environment against dictionary and other password attacks, the following practices should be followed:

- Do not allow passwords to be sent in cleartext.
- Encrypt the passwords with encryption algorithms or hashing functions.
- Employ one-time password tokens.
- Use hard-to-guess passwords.
- Rotate passwords frequently.
- Employ an IDS to detect suspicious behavior.
- Use dictionary cracking tools to find weak passwords chosen by users.
- Use special characters, numbers, and upper- and lowercase letters within the password.
- Protect password files.

Bruteforce Attacks

- Brute force is defined as “trying every possible combination until the correct one is identified.”
- The most effective way to uncover passwords is through a hybrid attack, which combines a dictionary attack and a brute force attack
- A brute force attack is also known as an exhaustive attack.
- These are usually used for wardialing in hopes of finding a modem that can be exploited to gain unauthorized access.

Countermeasures

For phone brute force attacks, auditing and monitoring of this type of activity should be in place to uncover patterns that could indicate a war dialing attack:

- Perform brute force attacks to find weaknesses and hanging modems.
- Make sure only necessary phone numbers are made public.
- Provide stringent access control methods that would make brute force attacks less successful.
- Monitor and audit for such activity.
- Employ an IDS to watch for suspicious activity.
- Set lockout thresholds.

Social Engineering

Social engineering is a collection of techniques used for manipulation of the natural human tendency to trust in order to obtain information that will allow a hacker to gain unauthorized access to a valued system and the information that resides on that system.
Forms of a Social engineering attack

- Physical: the workplace, the phone, your trash, and even on-line
- Psychological: Persuasion
- Reverse Social Engineering

Countermeasures

- Having proper security policies in place which addresses both physical and psychological aspects of the attack
- Providing proper training to employees, helpdesk personnel

c) Risk

Risk is the likelihood of a threat agent taking advantage of vulnerability and the corresponding business impact. Reducing vulnerability and/or threat reduces the risk.

E.g.: If a firewall has several ports open, there is a higher likelihood that an intruder will use one to access the network in an unauthorized method.

- Exposure

An exposure is an instance of being exposed to losses from a threat agent.

Vulnerability exposes an organization to possible damages.

E.g.:If password management is weak and password rules are not enforced, the company is exposed to the possibility of having users' passwords captured and used in an unauthorized manner.

- Countermeasure or Safeguard

It is an application or a software configuration or hardware configuration or a procedure that mitigates the risk.

E.g.: strong password management, a security guard, access control mechanisms within an operating system, the implementation of basic input/output system (BIOS) passwords, and security-awareness training.

The Relation between the Security Elements

Example 1

If a company has antivirus software but does not keep the virus signatures up-to-date, this is vulnerability. The company is vulnerable to virus attacks.

The threat is that a virus will show up in the environment and disrupt productivity.

The likelihood of a virus showing up in the environment and causing damage is the risk.

If a virus infiltrates the company's environment, then vulnerability has been exploited and the company is exposed to loss.

The countermeasures in this situation are to update the signatures and install the antivirus software on all computers

Threat Agent gives rise to Threat exploits Vulnerability leads to Risk can damage Assets and causes an Exposure can be counter measured by Safeguard directly effects Threat Agent

Example 2

Target: A bank contains money.

Threat: There are individuals who want, or need, additional money.

Vulnerability: The bank uses software that has a security flaw.

Exposure: 20% of the bank's assets are affected by this flaw.

Exploit: By running a small snippet of code (malware), the software can be accessed illegally.

Threat Agent: There are hackers who have learned how to use this malware to control the bank's software.

Exploitation: The hackers access the software using the malware and steal money.

Impact: The bank loses monetary assets, reputation, and future business.

Risk: The likelihood that a hacker will exploit the bank's software vulnerability and impact the bank's reputation and monetary resources.

Examples: Timeline chronicles ~ some cyber incidents out of 200 cyber incidents targeting financial institutions since 2007

- Beanstalk Farms cryptocurrency theft

On April 17, 2022, the decentralised finance platform Beanstalk Farms lost $180 million in a cryptocurrency heist.

- TransUnion SA data breach

March 17 2022 Credit bureau TransUnion SA suffered a cyber attack which saw around three million customer's data stolen by a criminal third party.

- Moscow Stock Exchange and Sberbank cyber attack

On February 28, 2022, the Moscow Stock Exchange and Sberbank, Russia’s largest lender, were hit by DDoS attacks that took their websites offline.

- Aon ransomware attack

On February 25, 2022, global insurance and reinsurance broker, Aon was hit by a ransomware attack, causing limited disruption to a number of their services.

- OCBC phishing scam

On December 23, 2021, around 790 banking customers of Singporean bank OCBC were targeted in a phishing scam resulting in a loss of at least $13.7 million.

- AscendEX hot wallet breach

On December 12, 2021, crypto exchange AscendEX lost $77.7 million in a breach of its hot wallet.

- BadgerDAO DeFi protocol hack

On December 2, 2021, decentralied finance ("DeFi") protocol BadgerDAO was hit by a cyber attack in which hackers stole $120.3 million in crypto.

- Ecuadorian Pichincha Bank disrupted by cyber attack

On October 10, 2021, Pichincha Bank in Ecuador was hit by a cyber attack that disrupted customers' access to bank services, including their online and mobile app tools.

- Taiwanese DeFi Platform hit by cyber attack

On August 30, 2021, Cream Finance, a Taiwanese decentralised finance platform, lost over $29 million in cryptocurrency assets to hackers.

- FBI Attributes Loss of $4 billion to Cybercrime

On March 17, 2021, the FBI released its Internet Crime Report 2020 which stated that American victims reported $4.2 billion in losses as a result of cybercrime and internet fraud to the FBI last year.

- Indonesian Fintech Data Breach

On October 31, Indonesian fintech company Cermati reported 2.9 million users' information was leaked and sold in a hacker forum.

- Payments Processor Juspay Data Leak

On August 18, 2020, payments processor Juspay's was hacked through a compromised server, resulting in the leak of over 100 million debit and credit card users.

- Finance Sector RDoS Campaign

On August 17, Akamai, a global content delivery network, reported an ongoing campaign of RDoS (Ransom DDoS) attacks targeting the financial sector and other businesses.

- NetWalker Ransomware Attacks

On August 4, 2020, McAfee reported that ransomware-as-a-service (RaaS) provider NetWalker had made $25 million over the previous five months through ransomware attacks.

- Norfund Business Email Compromise

On May 13, Norfund, Norway's state investment fund, was subject to a $10 million heist that involved business email compromise.

- South Korean and US Payment Card Leak

On April 9, 2020, a cache of 400,000 payment card records from banks in South Korea and the U.S. were uploaded to a well-known underground marketplace.

- Cardplanet Fraud

On November 13, 2019, the United States charged a Russian man for running ‘Cardplanet,’ a card trading platform worth almost $20 million USD that buys and sells stolen payment card details.

- Bank of Valletta

On February 13 2019, the Bank of Valletta (BOV), Malta’s largest and oldest bank, shut down operations after an attempted theft of €13 million.

- Bancomext Attempted SWIFT Heist

On January 9, 2018, attackers attempted to use fraudulent SWIFT transactions to steal $110 million from Bancomext, Mexico’s state-owned trade bank, but the money was ultimately recovered.

Costa Rican Financial Institution Attempted Theft

In January 2018, attackers attempted to steal $19 million from a private Costa Rican financial institution.

- Standard Bank Theft

On May 15, 2016, attackers stole $19 million from South Africa’s Standard Bank by making 14,000 withdrawals over 3 hours from 1,700 ATMs across Japan.

Guatemalan Financial Institution Theft

In December 2015, attackers stole $16 million from a Guatemalan financial institution.

- Bank of the West DDoS Attack

On Christmas Eve 2013, Bank of the West was the victim of a DDoS attack used to disguise $900,000 in fraudulent transfers out of accounts belonging to Ascent Builders, a Californian construction firm.

- Postbank Heist

From January 1-3 2020, hackers targeted Postbank, a division of the South African Post Office, breaching the organization's IT system and siphoning off cash into dummy accounts.

Risk Management Practices

A risk management team should have the ability and follow the best practices, some of them which include:

- Establishing a risk acceptance level as provided by senior management
- Documenting risk assessment processes and procedures
- Establishing proper procedures for identifying and mitigating risks
- Getting support from senior management for appropriate resource and fund allocation
- Defining contingency plans where assessments indicate that they are necessary
- Ensure that security-awareness training is provided for all staff members associated with information assets.
- Strive to establish improvement (or risk mitigation) in specific areas when necessary
- Should map legal and regulation compliancy requirements to control and implement requirements
- Develop metrics and performance indicators to be able to measure and manage various types of risks
- Identify and assess new risks as the environment and company changes
- Integrate IRM and the organization's change control process to ensure that changes do not introduce new vulnerabilities

Ways to deal with Risk

There are four basic ways of dealing with risks:

- Transfer it: If a company's total or residual risk is too high and it purchases an insurance then it is transfer of risk to the insurance company
- Reject it: If a company is in denial about its risk or ignore it, it is rejecting the risk
- Reduce it: If a company implements countermeasures, it is reducing the risk
- Accept it: If a company understands the risk and decides not to implement any kind of countermeasures it is accepting the risk. And this is actually what all computer systems boil down to. There is no way to mitigate the risk if the system is going to connect to the internet. Having only one user without any networking with others computer systems is the closet you can ever get to not having any risks.

Risk Assessment/Analysis

Risk analysis is a method of identifying vulnerabilities and threat and assessing the possible damage to determine where to implement security safeguards

Why Risk Analysis?

- ✓ To ensure that security is cost effective, relevant, timely, and responsive to threat.
- ✓ To provide a cost/benefit comparison, this compares the annualized cost of safeguards to the potential cost of loss.
- ✓ Help integrate the security program objectives with the company's business objectives and requirements
- ✓ To provide an economic balance between the impact of the threat and the cost of the countermeasure.

Analyze the risk

There are two approaches of analyzing risk

- ✓ Quantitative Approach
- ✓ Qualitative Approach

A Quantitative Approach to Risk Analysis

Quantitative analysis uses risk calculations that attempt to predict the level of monetary losses and percentage of chance for each type of threat.

Quantitative risk analysis also provides concrete probability percentages when determining the likelihood of threats.

Each element within the analysis (asset value, threat frequency, severity of vulnerability, impact damage, safeguard costs, safeguard effectiveness, uncertainty, and probability items) is quantified and entered into equations to determine total and residual risks.

Sample Steps for a Quantitative Risk Analysis

Step 1: Assign Value to Assets- For each asset, answer the following questions to determine its value

- What is the value of this asset to the company?
- How much does it cost to maintain?
- How much does it make in profits for the company?
- How much would it be worth to the competition?
- How much would it cost to re-create or recover?
- How much did it cost to acquire or develop?
- How much liability are you under pertaining to the protection of this asset?

Step 2: Estimate Potential Loss per Threat- To estimate potential losses posed by threats, answer the following questions:

- What physical damage could the threat cause and how much would that cost?
- How much loss of productivity could the threat cause and how much would that cost?
- What is the value lost if confidential information is disclosed?
- What is the cost of recovering from this threat?
- What is the value lost if critical devices were to fail?
- What is the single loss expectancy (SLE) for each asset, and each threat?

Step 3: Perform a Threat Analysis- Take the following steps to perform a threat analysis

- Gather information about the likelihood of each threat taking place from people in each department, past records, and official security resources that provide this type of data.
- Calculate the annualized rate of occurrence (ARO), which is how many times the threat can take place in a 12-month period.

Step 4: Derive the Overall Loss Potential per Threat-To derive the overall loss potential per threat, do the following:

- Combine potential loss and probability.
- Calculate the annualized loss expectancy (ALE) per threat by using the information calculated in the first three steps.
- Choose remedial measures to counteract each threat.
- Carry out cost/benefit analysis on the identified countermeasures.

Step 5: Reduce, Transfer, or Accept the Risk- For each risk, you can choose whether to reduce, transfer, or accept the risk:

Risk reduction methods

- Install security controls and components.
- Improve procedures.
- Alter environment.
- Provide early detection methods to catch the threat as it's happening and reduce the possible damage it can cause.
- Produce a contingency plan of how business can continue if a specific threat takes place, reducing further damages of the threat.
- Erect barriers to the threat.
- Carry out security-awareness training.

Risk transfer- Buy insurance to transfer some of the risk, for example.
Risk acceptance- Live with the risks and spend no more money toward protection.

Quantitative Risk Analysis Metrics

- Single loss expectancy (SLE) - The amount of loss due to a single occurrence of a threat.
- Annualized loss expectancy (ALE) - The estimated loss per annum.
- Exposure factor (EF) - Represents the percentage of loss a realized threat could have on a certain asset.
- Annualized rate of occurrence (ARO) – It is the value that represents the estimated frequency of a specific threat taking place within a one-year timeframe. It can range from 0.0 to 1.0.

Results of a Quantitative Risk Analysis

The following is a short list of what generally is expected from the results of a risk analysis

- Monetary values assigned to assets
- Comprehensive list of all possible and significant threats
- Probability of the occurrence rate of each threat
- Loss potential the company can endure per threat in a 12-month time span
- Recommended safeguards, countermeasures, and actions analysis.

A Qualitative Approach to Risk Analysis

- In Qualitative approach, we walk through different scenarios of risk possibilities and rank the seriousness of the threats and the validity of the different possible countermeasures.
- The Qualitative analysis techniques include judgment, best practices, intuition, and experience.
- Qualitative Risk Analysis Techniques
- Delphi -A group decision method used to ensure that each member gives an honest opinion of what he or she thinks the result to a particular threat will be. This method is used to obtain an agreement on cost, loss values, and probabilities of occurrence without individuals having to agree verbally.

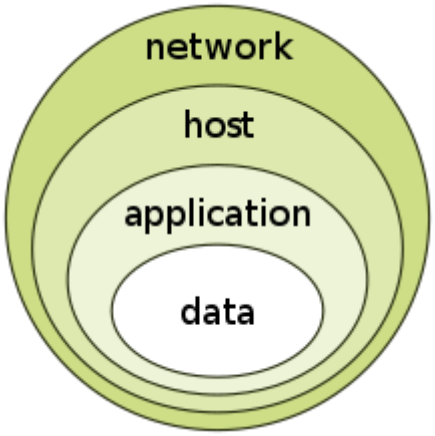
The risk analysis team will determine the best technique for the threats that need to be assessed and the culture of the company and individuals involved with the analysis.

Chapter three
INFORMATION SECURITY CONTROLS

Information security protects information and systems from malicious individuals or entities. It is a process of securing your personal data from unauthorized access, usage, revelation, interruption, modification, or deletion of data. The goal is to ensure the safety and privacy of critical data such as customer account details, financial data or intellectual property.

Information security must protect information throughout its lifespan, from the initial creation of the information on through to the final disposal of the information. The information must be protected while in motion and while at rest. During its lifetime, information may pass through many different information processing systems and through many different parts of information processing systems.

To fully protect the information during its lifetime, each component of the information processing system must have its own protection mechanisms.



The building up, layering on, and overlapping of security measures is called "defense in depth. In contrast to a metal chain, which is famously only as strong as its weakest link, the defense in depth strategy aims at a structure where, should one defensive measure fail, other measures will continue to provide protection

A very important component of information security is Cyber security.

Cyber security is how you protect against computer program, network and system attacks. Cyber security is not a one-and-done solution; it's a framework that evolves and adapts to a situation and includes oversight, prevention, and maintenance. Effective cyber security reduces the risk of a cyber-attack through the deliberate exploitation of systems, networks and technologies.

Cyber security can be broken down into three main pillars: **people, processes, and technology.** These three pillars of cyber security—people, processes, and technology—should all work together to build a sturdy defense network

- People in Cyber Security

People are the key components to consider when you administer and protect a company or individual's assets. They help drive the cyber security process, from multiple angles. They include decision makers, like C-suite executives, directors, and management; they also include the people who implement cyber security, like staff and third-party consultants.

- Cyber Security Processes

Processes are key to the implementation of an effective cyber security strategy. Processes are crucial in defining how the organisation's activities, roles and documentation are used to mitigate the risks to the organisation's information.

Processes and policy help provide the framework for governance and also define procedures that can be measured over time. This means processes are put into place to support the integrity of a security system. For example, a separation of duties ensures no single person is responsible for signing off on changes made to a product or system. Similarly, physical barriers like secure spaces, can ensure access and safety to hardware.

Processes also need to be continually reviewed: cyber threats change quickly and processes need to adapt with them. But processes are nothing if people don't follow them correctly.

- Technology with Cyber Security

Technology is the hardware and software that departments use to achieve reliable cyber security. These technologies hold data and information. Therefore, Data and information protection is the most technical and tangible of the three pillars. Data and information protection is the most technical and tangible of the three pillars. The data we gather comes from multiple sources, such as information technology (IT), operational technology (OT), personal data and operational data. It must be properly managed and protected every step of the way.

When discussing data and information, we must consider the CIA triad. The CIA triad refers to an information security model made up of the three main components: confidentiality, integrity and availability.

The three letters in "CIA triad" stand for Confidentiality, Integrity, and Availability. The CIA triad is a common model that forms the basis for the development of security systems. They are used for finding vulnerabilities and methods for creating solutions.

Availability

Availability is the protection of a system's ability to make software systems and data fully available when a user needs it (or at a specified time). The purpose of availability is to make the technology infrastructure, the applications and the data available when they are needed for an organizational process or for an organization's customers. while you need to make sure that your data can't be accessed by unauthorized users, you also need to ensure that it *can* be accessed by those who have the proper permissions.
Even if data is kept confidential and its integrity maintained, it is often useless unless it is available to those in the organization and the customers they serve. This means that systems, networks, and applications must be functioning as they should and when they should. Also, individuals with access to specific information must be able to consume it when they need to, and getting to the data should not take an inordinate amount of time.

If, for example, there is a power outage and there is no disaster recovery system in place to help users regain access to critical systems, availability will be compromised. Also, a natural disaster like a flood or even a severe snowstorm may prevent users from getting to the office, which can interrupt the availability of their workstations and other devices that provide business-critical information or applications. Availability can also be compromised through deliberate acts of sabotage, such as the use of denial-of-service (DoS) attacks or ransomware.

To ensure availability, organizations can use redundant networks, servers, and applications. These can be programmed to become available when the primary system has been disrupted or broken. You can also enhance availability by staying on top of upgrades to software packages and security systems. In this way, you make it less likely for an application to malfunction or for a relatively new threat to infiltrate your system. Backups and full disaster recovery plans also help a company regain availability soon after a negative event.

Integrity
Integrity involves making sure your data is trustworthy and free from tampering. The integrity of your data is maintained only if the data is authentic, accurate, and reliable.

For example, if your company provides information about senior managers on your website, this information needs to have integrity. If it is inaccurate, those visiting the website for information may feel your organization is not trustworthy. Someone with a vested interest in damaging the reputation of your organization may try to hack your website and alter the descriptions, photographs, or titles of the executives to hurt their reputation or that of the company as a whole.

Compromising integrity is often done intentionally. An attacker may bypass an intrusion detection system (IDS), change file configurations to allow unauthorized access, or alter the logs kept by the system to hide the attack. Integrity may also be violated by accident. Someone may accidentally enter the wrong code or make another kind of careless mistake. Also, if the company's security policies, protections, and procedures are inadequate, integrity can be violated without any one person in the organization accountable for the blame.

To protect the integrity of your data, you can use hashing, encryption, digital certificates, or digital signatures. For websites, you can employ trustworthy certificate authorities (CAs) that verify the authenticity of your website so visitors know they are getting the site they intended to visit.

A method for verifying integrity is non-repudiation, which refers to when something cannot be repudiated or denied. For example, if employees in your company use digital signatures when sending emails, the fact that the email came from them cannot be denied. Also, the recipient cannot deny that they received the email from the sender.

Consistency includes protection against unauthorized changes (additions, deletions, alterations, etc.) to data. The principle of integrity ensures that data is accurate and reliable and is not modified incorrectly, whether accidentally or maliciously.
Maintaining data in its correct state and preventing it from being improperly modified, either by accident or maliciously.

Confidentiality
Data is confidential when only those people who are authorized to access it can do so; to ensure confidentiality, you need to be able to identify who is trying to access data and block attempts by those without authorization.

Confidentiality involves the efforts of an organization to make sure data is kept secret or private. To accomplish this, access to information must be controlled to prevent the unauthorized sharing of data—whether intentional or accidental. A key component of maintaining confidentiality is making sure that people without proper authorization are prevented from accessing assets important to your business. Conversely, an effective system also ensures that those who need to have access have the necessary privileges.

For example, those who work with an organization's finances should be able to access the spreadsheets, bank accounts, and other information related to the flow of money. However, the vast majority of other employees—and perhaps even certain executives—may not be granted access. To ensure these policies are followed, stringent restrictions have to be in place to limit who can see what.

There are several ways confidentiality can be compromised. This may involve direct attacks aimed at gaining access to systems the attacker does not have the rights to see. It can also involve an attacker making a direct attempt to infiltrate an application or database so they can take data or alter it.

These direct attacks may use techniques such as man-in-the-middle (MITM) attacks, where an attacker positions themselves in the stream of information to intercept data and then either steal or alter it. Some attackers engage in other types of network spying to gain access to credentials. In some cases, the attacker will try to gain more system privileges to obtain the next level of clearance.

However, not all violations of confidentiality are intentional. Human error or insufficient security controls may be to blame as well. For example, someone may fail to protect their password—either to a workstation or to log in to a restricted area. Users may share their credentials with someone else, or

they may allow someone to see their login while they enter it. In other situations, a user may not properly encrypt a communication, allowing an attacker to intercept their information. Also, a thief may steal hardware, whether an entire computer or a device used in the login process and use it to access confidential information.

To fight against confidentiality breaches, you can classify and label restricted data, enable access control policies, encrypt data, and use multi-factor authentication (MFA) systems. It is also advisable to ensure that all in the organization have the training and knowledge they need to recognize the dangers and avoid them.

Ensures that the necessary level of secrecy is enforced at each junction of data processing and prevents unauthorized disclosure. This level of confidentiality should prevail while data resides on systems and devices within the network, as it is transmitted and once it reaches its destination.

Why Should You Use the CIA Triad?

The CIA triad provides a simple yet comprehensive high-level checklist for the evaluation of your security procedures and tools. An effective system satisfies all three components: confidentiality, integrity, and availability. An information security system that is lacking in one of the three aspects of the CIA triad is insufficient.

The CIA security triad is also valuable in assessing what went wrong—and what worked—after a negative incident. For example, perhaps availability was compromised after a malware attack such as ransomware, but the systems in place were still able to maintain the confidentiality of important information. This data can be used to address weak points and replicate successful policies and implementations.

When Should You Use the CIA Triad?

You should use the CIA triad in the majority of security situations, particularly because each component is critical. However, it is particularly helpful when developing systems around data classification and managing permissions and access privileges. You should also stringently employ the CIA triad when addressing the cyber vulnerabilities of your organization. It can be a powerful tool in disrupting the Cyber Kill Chain, which refers to the process of targeting and executing a cyberattack. The CIA security triad can help you hone in on what attackers may be after and then implement policies and tools to adequately protect those assets.