# Cyber law and professional Ethic

Dhiraj Bashyal
9851119570

# Thread Landscape

- Computer incidents
- Types of Exploits

# Thread Landscape –Introduction[1]

- Refer to a collection of threats in a particular domain or content, including data on vulnerable assets, threats, risks, threat actors , and observed treads.
- Encompasses all possible and identified cyber threats affecting a specific industry, and user group
- The threat landscape means **the entire scope of potential and recognized cybersecurity threats affecting user groups, organizations, specific industries, or a particular time**.
- Threat landscape analysis makes it possible to see potential information security problems facing a specific entity
  - — a company, an individual, or a whole sector
  - — and to take preventive measures by adopting a proactive approach to information security.

# Thread Landscape –Introduction[2]

- the threat landscape changes both over time and as a result of events with a significant impact on the organization, group of people, or sector for which the threat landscape is defined
- The following factors, among others, influence the threat landscape:
  - The emergence and discovery of vulnerabilities that provide cybercriminals with new attack opportunities;
  - The release of new software versions with additional functionality;
  - The development of new hardware platforms, as well as the emergence of new approaches to data processing, such as the use of cloud services or edge computing;
  - Global events such as the COVID-19 pandemic compelling organizations to make major changes to their infrastructure.

# Thread Landscape – Example[1]

- Cyber threats include **computer viruses, Denial of Service (DoS) attacks, and other attack vectors**
- Cyber threats faced significant challenges because of covid -19 pandemic.
  - Remote work has increased the attack  surface
  - necessary security team to cover a much larger than the previously required

# Thread Landscape – Example[2]

- common COVID-19 cyber threat, emails promise valuable information, but instead deliver dangerous malware for cyberespionage, ransomware installation, and credential theft
- Examples include:
  - **Ransomware** through a fake statement about coronavirus in Hong Kong, which referenced "Dr. Chuang Shuk-kwan, Head of the Communicable Disease Branch" to add an appearance of legitimacy
  - **Misleading "health and safety" emails**
- References
- https://www.boozallen.com/insights/covid-19/coronavirus-related-cyber-threats.html

# Computer incidents [1]

- An incident, in the context of information technology, is **an event that is not part of normal operations that disrupts operational processes**
- **Cyber incident means actions taken through the use of computer networks that result in a compromise or an actual or potentially adverse effect on an information system and/or the information residing therein.**

# Assignment  chapter 2

- Write down the top 10 cybersecurity incidents in 2022?
- Define Dos and D-Dos , Man in the Middle  and APT ?

# Security incidents in the cyber world[1]

1. Unauthorized attempts to access systems or data.
2. Insider threat.
3. Phishing attack.
4. Malware attack.
5. Denial-of-service (DoS) attack
6. Distributed Denial-of-service (DDoS) attack.

# Security incidents in the cyber world[2]

1. Man-in-the-middle (MitM) attack.
2. Password attack.
3. Sql injection
4. Advanced persistent threat (APT)
5. Web application attack

# Next day

- Exploits
- Types of Exploits

# Exploits[1]

- An exploit is a segment of code or a program that maliciously takes advantage of vulnerabilities or security flaws in software or hardware to infiltrate and initiate a denial-of-service (DoS) attack or install malware, such as spyware, ransomware, Trojan horses, worms, or viruses.
- An example of exploit is
  - **to pretend to befriend an intelligent student in class for the sole purpose of copying his homework**.
  - **SQL injection attacks, cross-site scripting and cross-site request forgery, as well as abuse of broken authentication code or security misconfigurations**.

# Exploits[2]

*In the illustration above, the window on the left is locked, so there's no vulnerability. The window on the right is open and vulnerable, but too high up to exploit. The window in the middle is open and vulnerable and, crucially, close enough to the ground to exploit.*

# Exploits[3]


When Attackers Target Vulnerabilities
HTTP://
OR
Attacker creates exploits to target software vulnerability
1. Exploits may arrive via:
- Attachment to email messages
- Comproised websites
- Social networking sites
2. Attacker may directly target vulnerable servers
OR
Users are lured into executing the exploit via social engineering techniques
Exploits may drop malware onto the vulnerable system or allow attackers remote control

# Exploits[4]

- What is the different between the malware and exploits ?
- Where do exploits come from?
- How do exploit attacks work?
- References
- https://www.avast.com/c-exploits

# Types of exploits

- Known exploits
  - **Known exploits** have already been discovered by cybersecurity researchers. Whether the known exploit is due to a vulnerability in the software, OS, or even hardware, developers can code patches to plug the hole. These patches are released to users as security updates. That's why it's crucial to keep your devices updated.
- Unknown exploits
  - **Unknown exploits** or zero-day exploits, in contrast, are created by cybercriminals as soon as they discover a vulnerability, and they use the exploit to attack victims on the same day. When a zero-day exploit attack happens, software developers and cybersecurity researchers have to scramble to figure out how the exploit works and how to patch the vulnerability.

# Exploits -Examples [1]

- **EternalBlue**
  - EternalBlue is one of the most famous — and most damaging — exploits out there. Originally developed by the NSA, EternalBlue was stolen by the Shadow Brokers hacking group and then leaked in March 2017. Although Microsoft discovered the leak and issued a security update to patch the vulnerability, many people and organizations failed to apply the patch in time. This allowed hackers to proceed with some of the most damaging cyberattacks in history, including WannaCry and NotPetya.
- **WannaCry**
  - WannaCry was the stuff of nightmares: a wormable attack that used the EternalBlue exploit to spread exponentially across computer networks, infecting 10,000 machines per hour in 150 countries. As ransomware, WannaCry encrypted computers, rendering them inaccessible — a huge issue for the national health services, governments, universities, and large corporations that WannaCry hit. Although WannaCry is no longer active, other exploits can still take advantage of EternalBlue to attack Windows users running outdated software — so make sure yours is updated.

# Exploits -Examples [2]

- **Petya and NotPetya**
  - Petya and its amusingly named successor, NotPetya, were ransomware strains (NotPetya also relied on the EternalBlue exploit). The Petyas caused huge damage by encrypting computers' master file table (MFT), rendering the machines completely unusable. And while there were ransom demands made, NotPetya could not be decrypted. So even if the users and organizations paid up, they never received anything in return. Experts estimate that Petya strains of ransomware caused over $10 billion in damage as they blew through banks and other corporations.

- **BlueKeep**
  - BlueKeep is an exploitable vulnerability in Microsoft Remote Desktop Protocol (RDP) that can allow attackers to log in to a victim's computer remotely. Microsoft raised the alarm about BlueKeep in May 2019, and issued a patch even for outdated operating systems such as Windows XP. That unusual step demonstrates the potential severity of BlueKeep: as it's another wormable exploit, many security researchers feared that BlueKeep would lead to the next devastating worldwide cyberattacks. As of this writing, BlueKeep has yet to amount to much, but it's still important to patch your system so you won't be caught in any future attacks.

# CIA Security Triad[1]

# CIA Security Triad[2]

- Confidentiality : keep information secret
- Integrity : Maintain the expected, accurate state of that information
- Availability :  Ensure your information and services are up and running

# Implementing CIA TRIAD at organizational, network application and end-user level

- There is no such thing as completely secure company
- If the attacker penetrates one layer of protection in tiered system, another act as the shield
- George W. Reynolds has presented layers of protective measures to stay secures from an attack the in shown in the figure

# Implementing CIA TRIAD at organizational, network application and end-user level

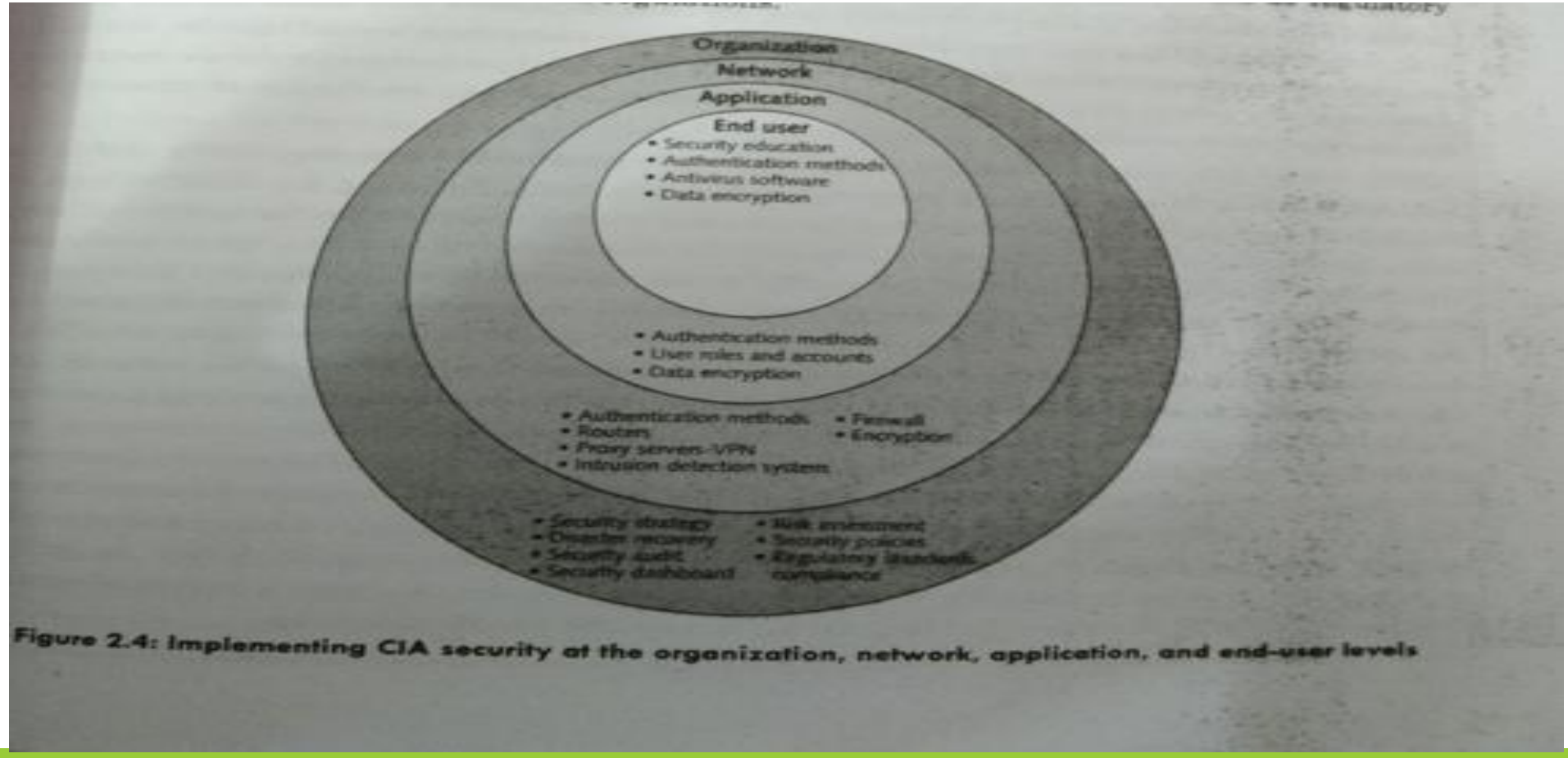



Figure 2.4: Implementing CIA security at the organization, network, application, and end-user levels

# Implementing CIA TRIAD at organizational Level

- Security strategy
- Disaster recovery
- Risk management
- Security policies
- Regulatory standards compliance
- Security dashboard

# Security strategy

That includes the organization primary security challenges and measure for dealing with them

A safe company has solid and well defined planed

# Disaster recovery

Good disaster plans will keep the organization operating despite disruptions of any sort, including power outages, IT system failures  etc.

A disaster recovery plan(DRP) outlines how a company will response to emergencies

# Security policies

The policies lists below are requires to implemented in all organization.

- Acceptable use policy
- Security awareness and training policy
- Change management policy
- Remote access policy
- Vendor management policy
- Password creation and management policy
- SPAM protection policy
- Vulnerability management policy etc.

# Security audit

Finding hazards improves the security holes in IT  organizations

Security audit includes vulnerability scans, which check for security holes in IT systems as well as doing penetration tests to gain unauthorized access to the applications, system and networks.

Security audit provides various benefits such as:

- Evaluates the existing setup and practices and uses the audit finding set a benchmark for business
- Reduces hacker treats
- And so on

# Regulatory standards compliance

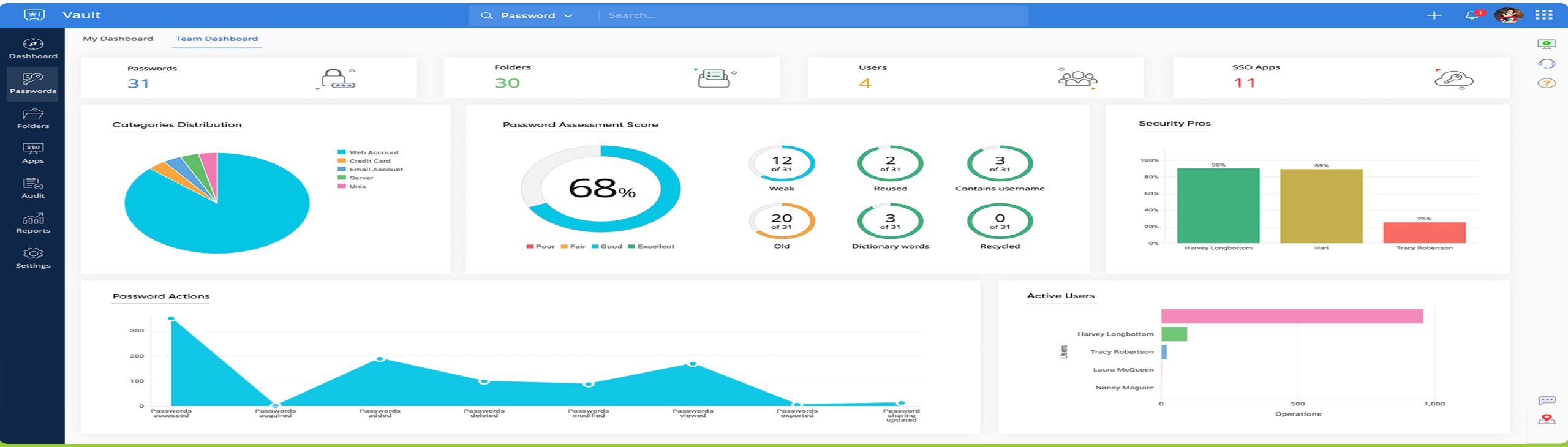
Refers to a collection of rules that a business must abide by to operation legally.

Regulatory compliance is **an organization's adherence to laws, regulations, guidelines and specifications relevant to its business processes**.

# Security dashboard

Security Dashboard **lets you view the health of your security settings**.

Find information on attackers,and victims and view what attacks and packets the appliance blocked over time.



# Implementing CIA TRIAD at Network Application

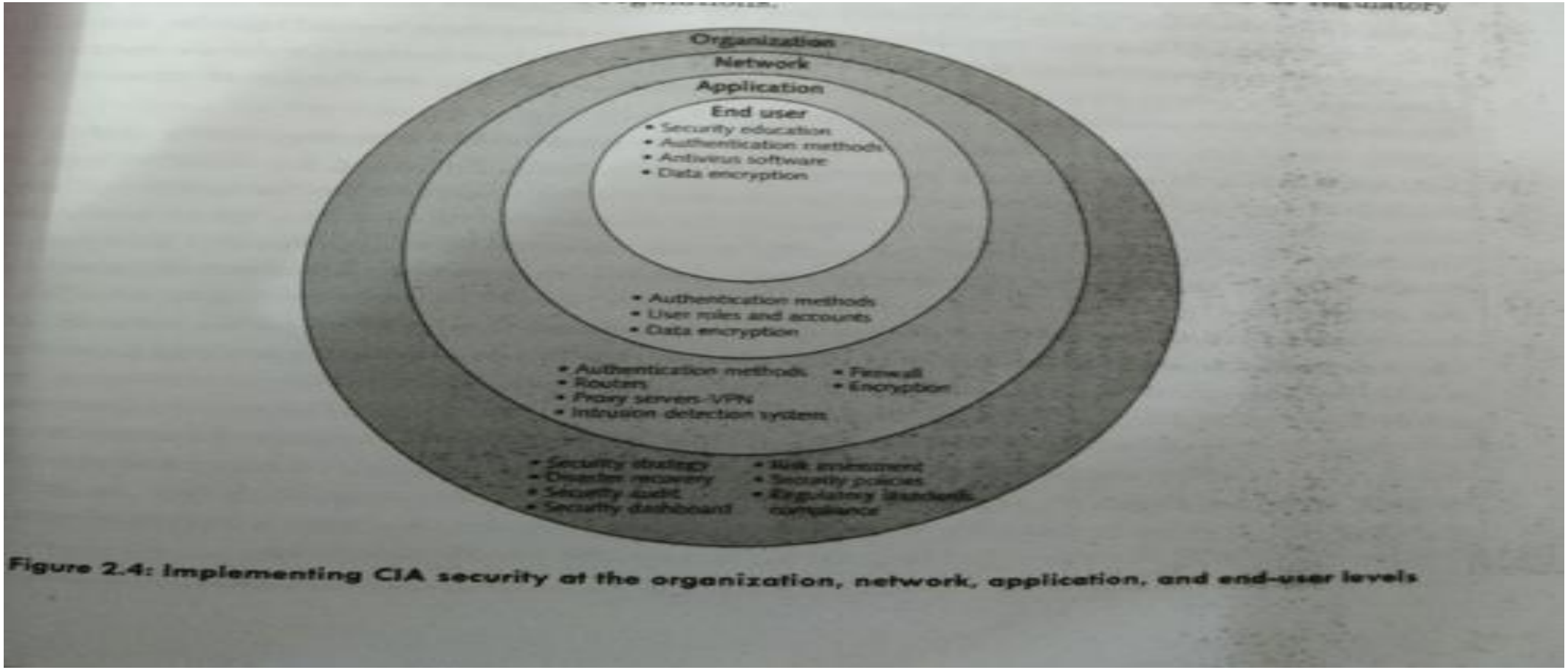



Figure 2.4: Implementing CIA security at the organization, network, application, and end-user levels

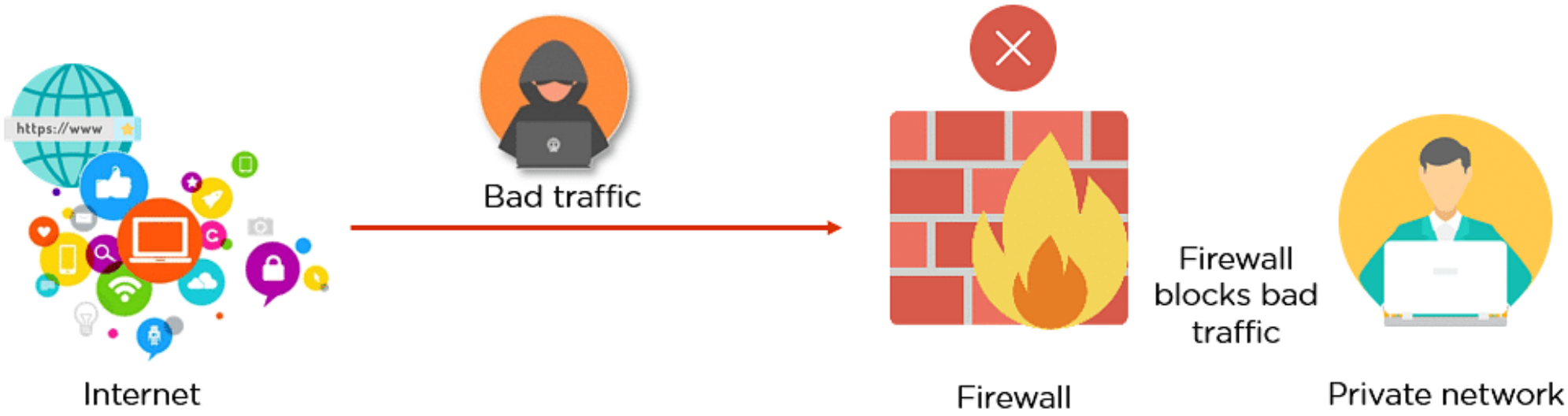
# Implementing CIA TRIAD at Network Application

- Firewall
- Routers
- Encryption
- Proxy server and virtual private networks
- Intrusion detection system

# Firewall

- A Firewall is **a network security device that monitors and filters incoming and outgoing network traffic based on an organization's previously established security policies**
- Firewalls are **network security systems that prevent unauthorized access to a network**.
- A firewall can **help protect your computer and data by managing your network traffic**
- A firewall validates access by assessing this incoming traffic for anything malicious like hackers and malware that could infect your computer

# Firewall


https://www
Bad traffic
Internet
Firewall
Firewall blocks bad traffic
Private network

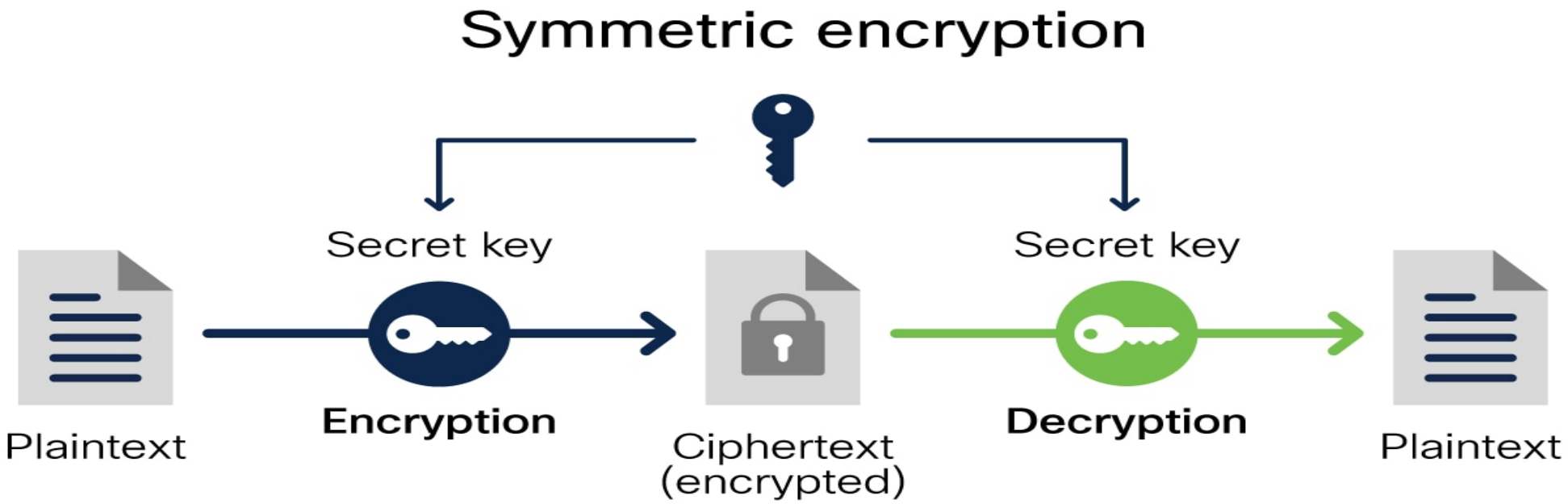
# Routers

- A **router** is a networking device that forwards data packets between computer networks.
- **Routers** perform the traffic directing functions on the Internet.
- Routers **bring the Internet to your devices**
- The **router** is a physical or virtual internetworking device that is designed to receive, analyze, and forward data packets between computer networks.
- It serves two primary functions: managing traffic between these networks by forwarding data packets to their intended IP addresses, and allowing multiple devices to use the same Internet connection.

# Encryption

- Encryption is **the method by which information is converted into secret code that hides the information's true meaning**
- **Encryption** is the security method of encoding data from plaintext to ciphertext, which can only be decrypted by the user with the **encryption** key.
- Encryption **ensures effective security where information cannot be intercepted and used to hinder emergency response or endanger responders and the public**.

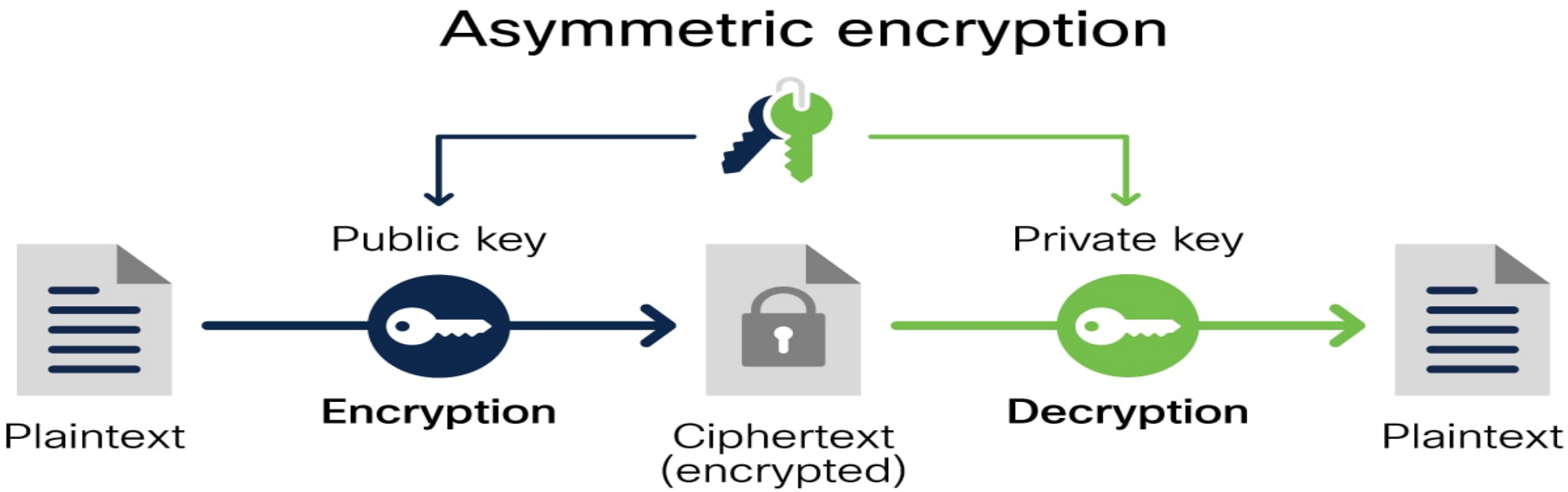
# Symmetric encryption[1]



# Symmetric encryption[2]

- Symmetric encryption uses the same key for encryption and decryption.
- Because it uses the same key, symmetric encryption can be more cost effective for the security it provides.
- That said, it is important to invest more in securely storing data when using symmetric encryption.

# Asymmetric encryption[1]



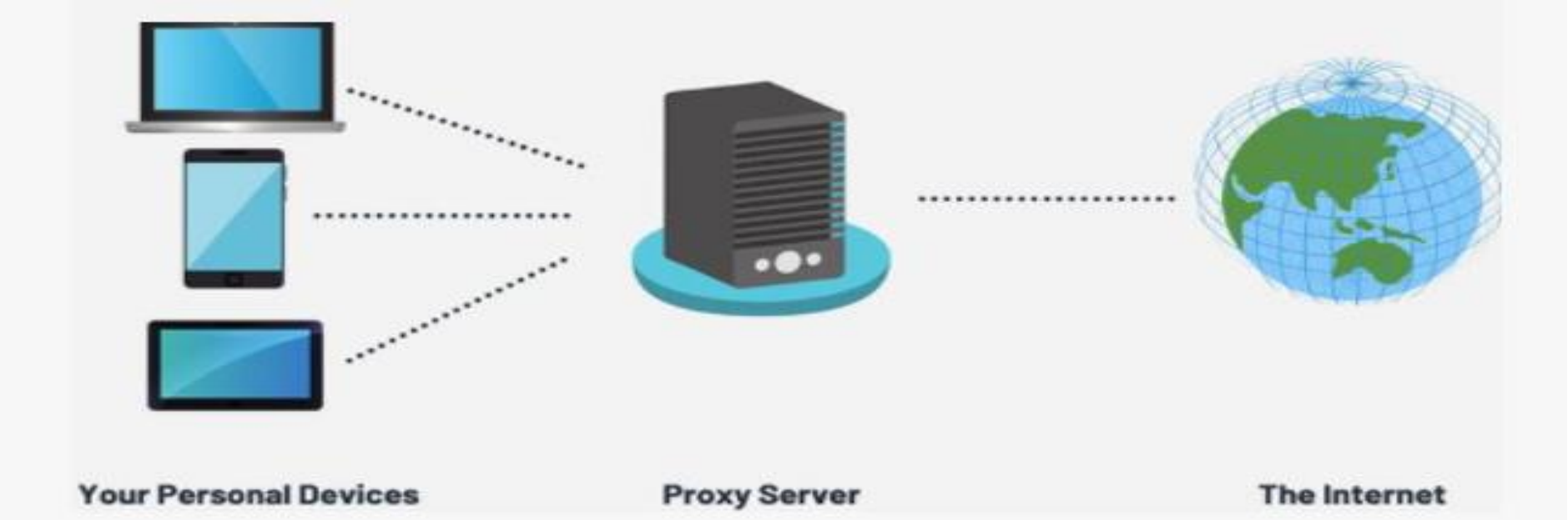
# Asymmetric encryption[2]

- Asymmetric encryption uses two separate keys: a public key and a private key.
- Often a public key is used to encrypt the data while a private key is required to decrypt the data.
- The private key is only given to users with authorized access.
- As a result, asymmetric encryption can be more effective, but it is also more costly.

# Proxy server and virtual private networks

A **proxy server** is a system or router that provides a gateway between users and the internet.

Therefore, it helps prevent cyber attackers from entering a private network.



# Intrusion detection system

An **Intrusion Detection System (IDS)** is a system that monitors **network traffic** for suspicious activity and issues alerts when such activity is discovered.

- • passive monitoring solution for detecting cyber security threats/ breaches.
- • IDS designed to aid in mitigating damage caused by hacking.
- • IDS generates an alert – notifies security personnel to investigate the incident and take remediative action.

Basic intent behind IDS: spot something suspicious on NW/system and sound alarm.

• May look for data bits that indicate questionable activity or monitor system logs.

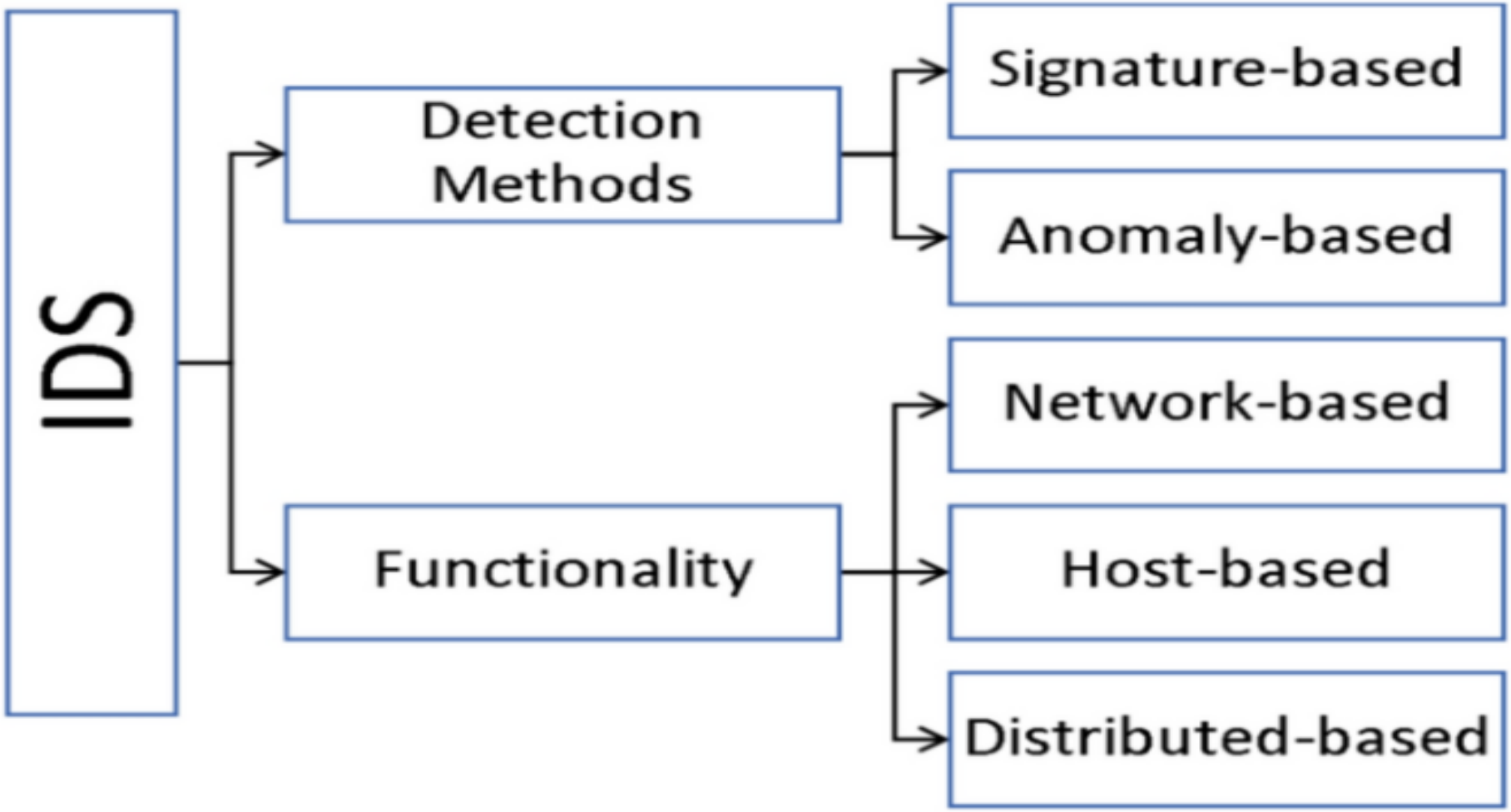
• Events that sound alarm – may not be an intrusion; any abnormal activity may trigger, depending on configuration.

# Intrusion detection system

All IDS have three things in common:

- Sensors:
  - – collect traffic and user activity data and sends to analyzer.
- Analyzer:
  - – Looks for suspicious activity.
- Administrator Interface:
  - – If analyzer detects suspicious activity, sends an alert to the Admin Interface.

# IDS Classification



# Host based Intrusion Detection Systems (HIDS)

– monitors the host's network traffic, running processes, logs, etc., or

– Installed on individual workstations/ servers

– Watches for abnormal activity NIDs understands and monitors NW traffic, HIDS monitors the computer only on which it is installed.

– Generally, HIDS installed on critical servers only due to administrative overheads.

# Network Intrusion Detection Systems (NIDS)

– identify threats to the entire network.

– Uses sensors to monitor all NW traffic

– Cannot see the activities within the computer itself.

# Based on how they identify potential threats/ Detection Methods

- **Signature based** – uses a library of signatures of known threats to identify them.
  - • Pattern matching
  - • Stateful matching
- **Anomaly based**
  - – builds a model of “normal” behavior of the protected system and reports on any deviations
  - .• Statistical anomaly based
  - • Protocol anomaly based
  - • Traffic anomaly based

# Knowledge or Signature based IDS

- Knowledge is gained by sensors about how specific attacks are carried out.
- Each identified attack has a signature
- Most popular IDS today.
- Effectiveness depends on regularly updating signature database.
- May not be able to uncover new types of attacks.

# Anomaly based IDS

Anomaly-based IDSes **typically work by taking a baseline of the normal traffic and activity taking place on the network**.

They can measure the present state of traffic on the network against this baseline in order to detect patterns that are not present in the traffic normally.

For example, **if large sums of money are spent one after another within one day and it is not your typical behavior, a bank can block your card**.

# Implementing CIA TRIAD at Network Application

Application level

- Application method
- Authentication factor
- User roles and accounts
- Data encryption

# Implementing CIA TRIAD at Application

Security education

Authentication methods

- Single factor Authentication
- Two factor Authentication

Antivirus software

Data encryption

# Response to Cyber Attack

- Over the past years, the size and magnitude of cyber security breaches have increased.
- More often we tend to underestimate the possibility of falling prey to a cyber attack. Small businesses feel like they're too small to be attacked and larger companies like to believe that they have all the right protective measures in place to stay safe from cyber attacks
- In reality, the amount of security in place or the scale of a business does not decrease the chances of falling prey to a cyber attack.
- Companies should have a clear understanding of how to respond and recover from a cyber-attack.
- The default should be to turn to your cyber security incident response plan to take action immediately and better contain or reduce the impact of a cyber-attack.

# Incident Notification

Notification incident generally includes a significant computer-security incident that disrupts or degrades, or is reasonably likely to disrupt or degrade, the viability of the bank's operations; results in customers being unable to access their deposit and other accounts;

# Protection of Evidence and activity logs

Incident Containment

Eradication

Incident follow-up

Using a managed security security provider (MSSP

# Eradication

- Eradication is **a critical phase in the incident response process**
- Thorough recovery from security incidents requires the full removal of any malicious code or other threats that were introduced to the environment during the incident. This is the purpose of the eradication phase.
- But while eliminating threats may seem like the most obvious response to an incident, eradication is one of many necessary phases in an effective incident response program.

# Incident Response Process Phases

Security programs are designed to meet the unique needs of each organization, so the exact phases of incident response may differ slightly from one security program to the next. But the incident response is usually broken down into seven phases. These phases include:

**Preparation** – Function with the expectation that an incident will eventually occur and prepare accordingly. Define roles, delegate tasks, and create a plan for responding to different levels of incidents so that everyone knows what to do before one happens.

**Detection** – Define and implement measures to detect threats so they can be identified and prioritized appropriately.

**Containment** – Quarantine any threats identified during the detection phase to mitigate the impact on the environment.

# Incident Response Process Phases

**Investigation** – Once the threat has been contained, find and document the cause of the incident.

**Eradication** – Remove any malware or other threats that were introduced to the environment in order of priority.

**Recovery** – Do any necessary data and asset recovery to restore systems and assets to their pre-incident state.

**Follow-up** – Review the impact of the incident and the results of the response process, and consider whether any improvements are needed to be better prepared for future incident response.

# Using a managed security security provider (MSSP)

Managed security service providers (MSSP) **deliver management and outsourced monitoring of systems and security devices**. An MSSP can also handle upgrades, system changes, and modification.

A managed security service provider (MSSP) is an information technology (IT) service provider that sells security services to businesses.

The role of an MSSP is to help protect businesses from security threats, whether that means providing software and services that keep company data safe or building a network of security experts who can respond to attacks as they happen.

MSSPs provide cybersecurity monitoring and management, which may include virus and spam blocking, intrusion detection, firewalls and virtual private network (VPN) management. MSSPs also handle matters such as system changes, modifications and upgrades.

# Using a managed security security provider (MSSP)

There are six main categories of managed security services, including:

- on-site consulting;
- perimeter management of the client's network;
- product resale;
- managed security monitoring;
- penetration testing and vulnerability assessments; and
- compliance monitoring.

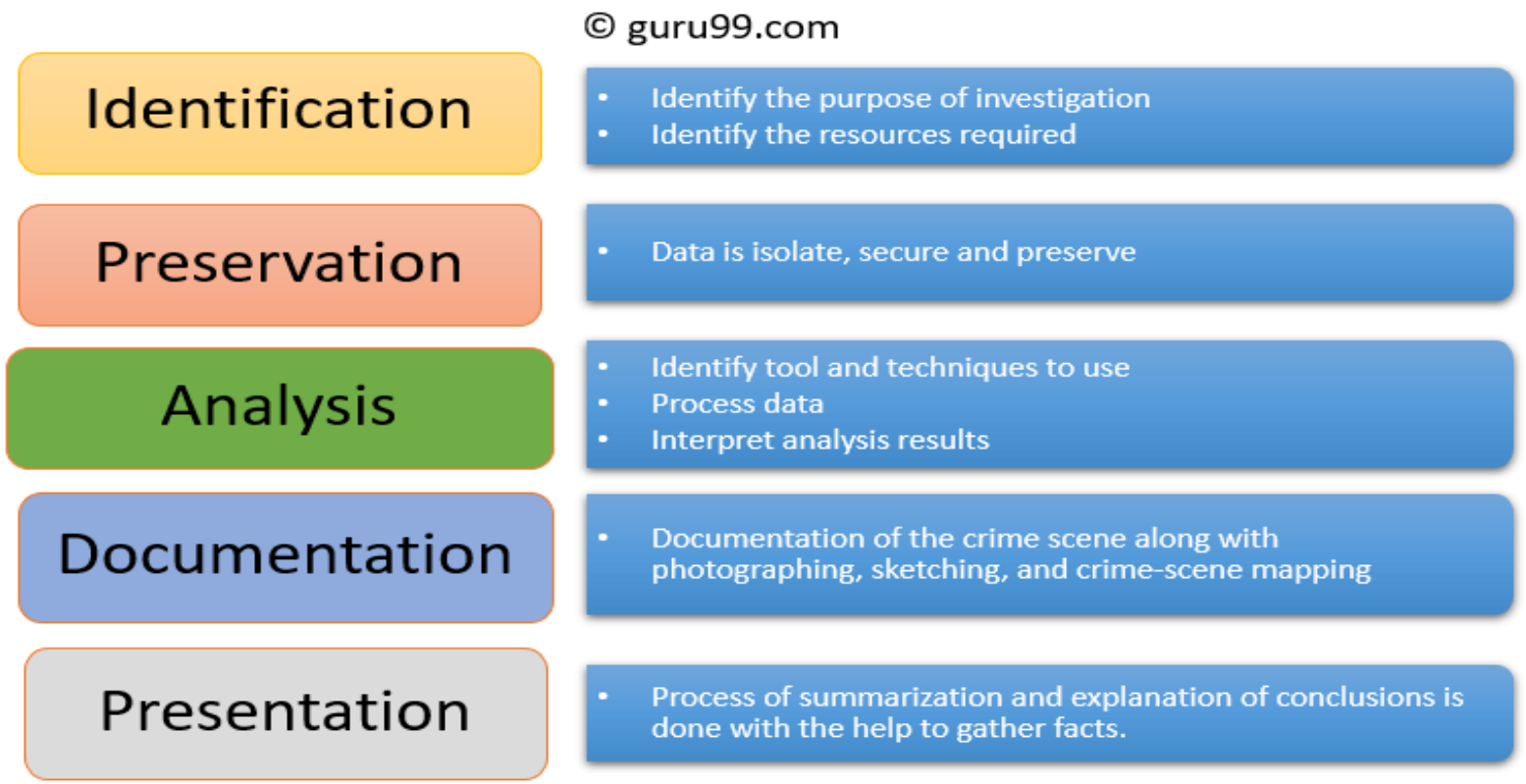
# Computer forensics

- Computer forensics is the application of investigation and analysis techniques to gather and preserve evidence from a particular computing device in a way that is suitable for presentation in a court of law.
- The goal of computer forensics is to perform a structured investigation and maintain a documented chain of evidence to find out exactly what happened on a computing device and who was responsible for it.

# Digital Forensics

- Digital Forensics is defined as the process of preservation, identification, extraction, and documentation of computer evidence which can be used by the court of law.
- It is a science of finding evidence from digital media like a computer, mobile phone, server, or network. It provides the forensic team with the best techniques and tools to solve complicated digital-related cases.
- Digital Forensics helps the forensic team to analyzes, inspect, identifies, and preserve the digital evidence residing on various types of electronic devices.

# Process of Digital forensics



# Process of Digital forensics

**Identification**

It is the first step in the forensic process. The identification process mainly includes things like what evidence is present, where it is stored, and lastly, how it is stored (in which format).

Electronic storage media can be personal computers, Mobile phones, PDAs, etc.

**Preservation**

In this phase, data is isolated, secured, and preserved. It includes preventing people from using the digital device so that digital evidence is not tampered with.

**Analysis**

In this step, investigation agents reconstruct fragments of data and draw conclusions based on evidence found. However, it might take numerous iterations of examination to support a specific crime theory.

# Process of Digital forensics

**Documentation**

In this process, a record of all the visible data must be created. It helps in recreating the crime scene and reviewing it. It Involves proper documentation of the crime scene along with photographing, sketching, and crime-scene mapping.

**Presentation**

In this last step, the process of summarization and explanation of conclusions is done.

However, it should be written in a layperson's terms using abstracted terminologies. All abstracted terminologies should reference the specific details.

# Cyber Law

- Cyber Law also called IT Law is **the law regarding Information-technology including computers and the internet**.
- It is related to legal informatics and supervises the digital circulation of information, software, information security, and e-commerce.

**Importance of Cyber Law:**

- It covers all transactions over the internet.
- It keeps eye on all activities over the internet.
- It touches every action and every reaction in cyberspace.

# Cyber law in Nepal

(study from book)

# Electronics transaction act in Nepal

To pirate ,Destroy or alter computer source code

Unauthorized access in computer material

Damage to any computer and information system

Publication of illegal material in electronic form

Confidentiality to divulge

To  commit computer fraud

Abetment to commit computer related offence

Punishment in an offence committed outside Nepal

Confiscation

# End of chapter 2

# Thank you !!!!