

Cybersecurity Fundamentals

Lecture 2: Introduction to Cybersecurity Concepts

CYB 670

Cybersecurity Fundamentals

Presented by

Dr. Mohammad Alkhatib



Outline

The module covers the basics of cybersecurity including:

- The Importance and challenges in Cybersecurity,
- Cyberspace, Cyber threats, Cyberwarfare,
- CIA Triad, Threats, and attacks (such as Eavesdropping, Alteration, Denial-of service, Masquerading, Repudiation, Correlation and traceback),
- Cyber Terrorism,
- Cyber Security of Critical Infrastructure,
- Cybersecurity - Organizational Implications.

The Definition of Cybersecurity

- **Cybersecurity** refers to the body of technologies, processes, and practices designed to protect networks, devices, programs, and data from attack, damage, or unauthorized access. Cyber security may also be referred to as information technology security.
- **Cybersecurity** is the practice of protecting critical systems and sensitive information from digital attacks ([IBM](#))
- **Cybersecurity** is the protection of internet-connected systems such as hardware, software and data from cyberthreats ([TeachTarget](#))
- **Cybersecurity** is the application of technologies, processes and controls to protect systems, networks, programs, devices and data from cyber attacks. ([itgovernance.co.uk](#))



Can be divided into a few common categories:

- **Network security** is the practice of securing a computer network from intruders, whether targeted attackers or opportunistic malware.
- **Application security** focuses on keeping software and devices free of threats. A compromised application could provide access to the data its designed to protect. Successful security begins in the design stage, well before a program or device is deployed.
- **Information security** protects the integrity and privacy of data, both in storage and in transit.



❖ *Can be divided into a few common categories:*

- **Operational security** includes the processes and decisions for handling and protecting data assets. The permissions users have when accessing a network and the procedures that determine how and where data may be stored or shared all fall under this umbrella.
- **Disaster recovery and business continuity** define how an organization responds to a cyber-security incident or any other event that causes the loss of operations or data. Disaster recovery policies dictate how the organization restores its operations and information to return to the same operating capacity as before the event. Business continuity is the plan the organization falls back on while trying to operate without certain resources.



- *Can be divided into a few common categories:*
- **End-user education** addresses the most unpredictable cyber-security factor: people. Anyone can accidentally introduce a virus to an otherwise secure system by failing to follow good security practices. Teaching users to delete suspicious email attachments, not plug in unidentified USB drives, and various other important lessons is vital for the security of any organization.
(www.kaspersky.com)



Cyber security is important because it protects all categories of data from theft and damage. This includes sensitive data, personally identifiable information (PII), protected health information (PHI), personal information, intellectual property, data, and governmental and industry information systems.

Why is Cyber Awareness Important?

- Cyber crime is a growing trend
- Raise awareness of threats
- As with most crimes the police can't tackle this problem alone
- To encourage reporting
- Promote Government backed scheme 'Cyber Essentials'
- Cyber crime is massively under reported.



- For effective cyber security, an organization needs to coordinate its efforts throughout its entire information system.

Elements of cyber encompass all of the following:

- ❖ **Network security:** The process of protecting the network from unwanted users, attacks and intrusions.
- ❖ **Application security:** Apps require constant updates and testing to ensure these programs are secure from attacks.
- ❖ **Endpoint security:** Remote access is a necessary part of business, but can also be a weak point for data. Endpoint security is the process of protecting remote access to a company's network.
- ❖ **Data security:** Inside of networks and applications is data. Protecting company and customer information is a separate layer of security.
- ❖ **Identity management:** Essentially, this is a process of understanding the access every individual has in an organization.



➤ Elements of cyber encompass all of the following:

- ❖ **Database and infrastructure security:** Everything in a network involves databases and physical equipment. Protecting these devices is equally important.
- ❖ **Cloud security:** Many files are in digital environments or “the cloud”. Protecting data in a 100% online environment presents a large amount of challenges.
- ❖ **Security for mobile devices:** Cell phones and tablets involve virtually every type of security challenge in and of themselves.
- ❖ **Disaster recovery/business continuity planning:** In the event of a security breach, natural disaster or other event data must be protected and business must go on. For this, you’ll need a plan.
- ❖ **End-user education:** Users may be employees accessing the network or customers logging on to a company app. Educating good habits (password changes and having a strong password, 2-factor authentication, etc.) is an important part of cybersecurity.

Challenges of Cybersecurity



- ❖ The most difficult challenge in cyber security is the ever-evolving nature of security risks themselves. Traditionally, organizations and the government have focused most of their cyber security resources on perimeter security to protect only their most crucial system components and defend against known threats. Today, this approach is insufficient, as the threats advance and change more quickly than organizations can keep up with. As a result, advisory organizations promote more proactive and adaptive approaches to cyber security.

- **Cyberspace** is more than the internet, including not only hardware, software, data and information systems, but also people and social interaction within these networks and the whole infrastructure.
- **The International Telecommunication Union (ITU)** uses the term to describe the “systems and services connected either directly to or indirectly to the internet, telecommunications and computer networks.”
- **The International Organisation for Standardisation (ISO)** defining cyber as “the complex environment resulting from the interaction of people, software and services on the internet by means of technology devices and networks connected to it, which does not exist in any physical form.”



- **A cyber or cybersecurity threat** is a malicious act that seeks to damage data, steal data, or disrupt digital life in general. Cyber threats include computer viruses, data breaches, Denial of Service (DoS) attacks, and other attack vectors.
- **Cyber threats** also refer to the possibility of a successful cyber attack that aims to gain unauthorized access, damage, disrupt, or steal an information technology asset, computer network, intellectual property or any other form of sensitive data. Cyber threats can come from within an organization by trusted users or from remote locations by unknown parties.



Cyber threats come from numerous threat actors including:

- Hostile Nation-States.
- Corporate Spies and Organized Crime Organizations
- Terrorist Groups
- Hacktivists (across political ideals and issues)
- Disgruntled Insiders
- Hackers
- Natural Disasters
- Accidental Actions of Authorized Users

Common cyber threats include:

❖ **Malware**

Malware is software that does malicious tasks on a device or network such as corrupting data or taking control of a system.

❖ **Spyware**

Spyware is a form of malware that hides on a device providing real-time information sharing to its host, enabling them to steal data like bank details and passwords.

❖ **Phishing Attacks**

Phishing is when a cybercriminal attempts to lure individuals into providing sensitive data such as personally identifiable information (PII), banking and credit card details and passwords.

❖ **Distributed Denial of Service (DDoS) Attacks**

Distributed denial of service attacks aim to disrupt a computer network by flooding the network with superfluous requests to overload the system and prevent legitimate requests being fulfilled.

Common cyber threats include:

❖ Ransomware

Ransomware is a type of malware that denies access to a computer system or data until a ransom is paid.

❖ Zero-Day Exploits

A zero-day exploit is a flaw in software, hardware or firmware that is unknown to the party or parties responsible for patching the flaw.

❖ Advanced Persistent Threats

An advanced persistent threat is when an unauthorized user gains access to a system or network and remains there without being detected for an extended period of time.

❖ Trojans

A trojan creates a backdoor in your system, allowing the attacker to gain control of your computer or access confidential information.

Common cyber threats include:

❖ **Wiper Attacks**

A wiper attack is a form of malware whose intention is to wipe the hard drive of the computer it infects.

❖ **Intellectual Property Theft**

Intellectual property theft is stealing or using someone else's intellectual property without permission.

❖ **Theft of Money**

Cyber attacks may gain access to credit card numbers or bank accounts to steal money.

❖ **Data Manipulation**

Data manipulation is a form of cyber attack that doesn't steal data but aims to change the data to make it harder for an organization to operate.

❖ **Data Destruction**

Data destruction is when a cyber attacker attempts to delete data.

Types of Cyber Security Threats

Common cyber threats include:

❖ **Man-in-the-Middle Attack (MITM Attack)**

A MITM attack is when an attacker relays and possibly alters the communication between two parties who believe they are communicating with each other.

❖ **Drive-by Downloads**

A drive-by download attack is a download that happens without a person's knowledge often installing a computer virus, spyware, or malware.

❖ **Malvertising**

Malvertising is the use of online advertising to spread malware.

❖ **Rogue Software**

Rogue software is malware that is disguised as real software.

❖ **Unpatched Software**

Unpatched software is software that has a known security weakness that has been fixed in a later release but not yet updated.

Common cyber threats include:

❖ Data Centre Disrupted by Natural Disaster

The data centre your software is housed on could be disrupted by a natural disaster like flooding.

❖ SQL Injection

A Structured Query Language (SQL) injection is a type of cyber attack that results from inserting malicious code into a server that uses SQL. When infected, the server releases information. Submitting the malicious code can be as simple as entering it into a vulnerable website search box.

❖ Password Attacks

With the right password, a cyber attacker has access to a wealth of information. Social engineering is a type of password attack that Data Insider defines as “a strategy cyber attackers use that relies heavily on human interaction and often involves tricking people into breaking standard security practices.” Other types of password attacks include accessing a password database or outright guessing.



- **Cyber warfare** is usually defined as a cyber attack or series of attacks that target a country. It has the potential to wreak havoc on government and civilian infrastructure and disrupt critical systems, resulting in damage to the state and even loss of life.

- **Here are some of the main types of cyber warfare attacks**



Espionage



Sabotage



Denial-of-service
(DoS) Attacks



Electrical
Power Grid



Propaganda
Attacks



Economic
Disruption



Surprise
Attacks



- **Here are some of the main types of cyber warfare attacks**

- **Espionage**

Refers to monitoring other countries to steal secrets. In cyber warfare, this can involve using botnets or spear phishing attacks to compromise sensitive computer systems before exfiltrating sensitive information.

- **Sabotage**

Government organizations must determine sensitive information and the risks if it is compromised. Hostile governments or terrorists may steal information, destroy it, or leverage insider threats such as dissatisfied or careless employees, or government employees with affiliation to the attacking country.

- **Denial-of-service (DoS) Attacks**

DoS attacks prevent legitimate users from accessing a website by flooding it with fake requests and forcing the website to handle these requests. This type of attack can be used to disrupt critical operations and systems and block access to sensitive websites by civilians, military and security personnel, or research bodies.



- **Here are some of the main types of cyber warfare attacks**

- **Electrical Power Grid**

Attacking the power grid allows attackers to disable critical systems, disrupt infrastructure, and potentially result in bodily harm. Attacks on the power grid can also disrupt communications and render services such as text messages and communications unusable.

- **Propaganda Attacks**

Attempts to control the minds and thoughts of people living in or fighting for a target country. Propaganda can be used to expose embarrassing truths, spread lies to make people lose trust in their country, or side with their enemies.



- Here are some of the main types of cyber warfare attacks

- **Economic Disruption**

Most modern economic systems operate using computers. Attackers can target computer networks of economic establishments such as stock markets, payment systems, and banks to steal money or block people from accessing the funds they need.

- **Surprise Attacks**

These are the cyber equivalent of attacks like Pearl Harbor and 9/11. The point is to carry out a massive attack that the enemy isn't expecting, enabling the attacker to weaken their defenses. This can be done to prepare the ground for a physical attack in the context of hybrid warfare.

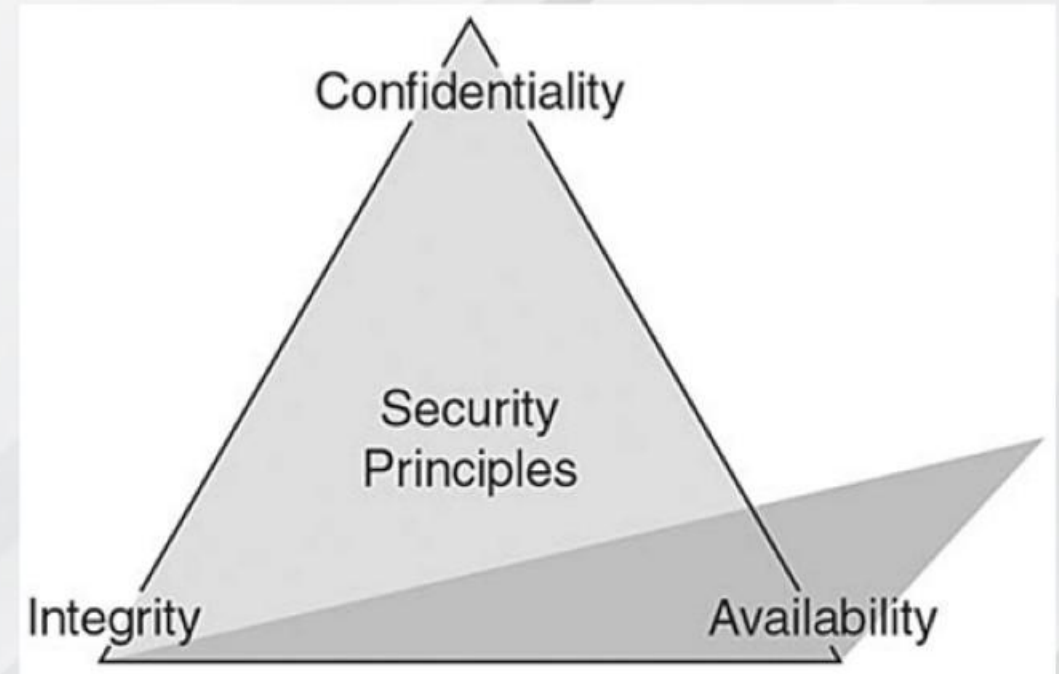


- ❖ **Cyber terrorism** is often defined as any premeditated, politically motivated attack against information systems, programs and data that threatens violence or results in violence. The definition is sometimes expanded to include any cyber attack that intimidates or generates fear in the target population.
- ❖ The nature of cyberterrorism covers conduct involving computer or Internet technology that:
 - 1) is motivated by a political, religious or ideological cause
 - 2) is intended to intimidate a government or a section of the public to varying degrees
 - 3) seriously interferes with infrastructure

The CIA Triad

The primary goals and objectives of security are contained within the *CIA Triad*, as shown below:

- **Confidentiality** means protection from unauthorized access
- **Integrity** means protection from unauthorized modification,
- **Availability** means protection from disruptions in access.



Security Attacks

- **Interruption:**
- This is an attack on availability
- **Interception:**
- This is an attack on confidentiality
- **Modification:**
- This is an attack on integrity
- **Fabrication:**
- This is an attack on authenticity

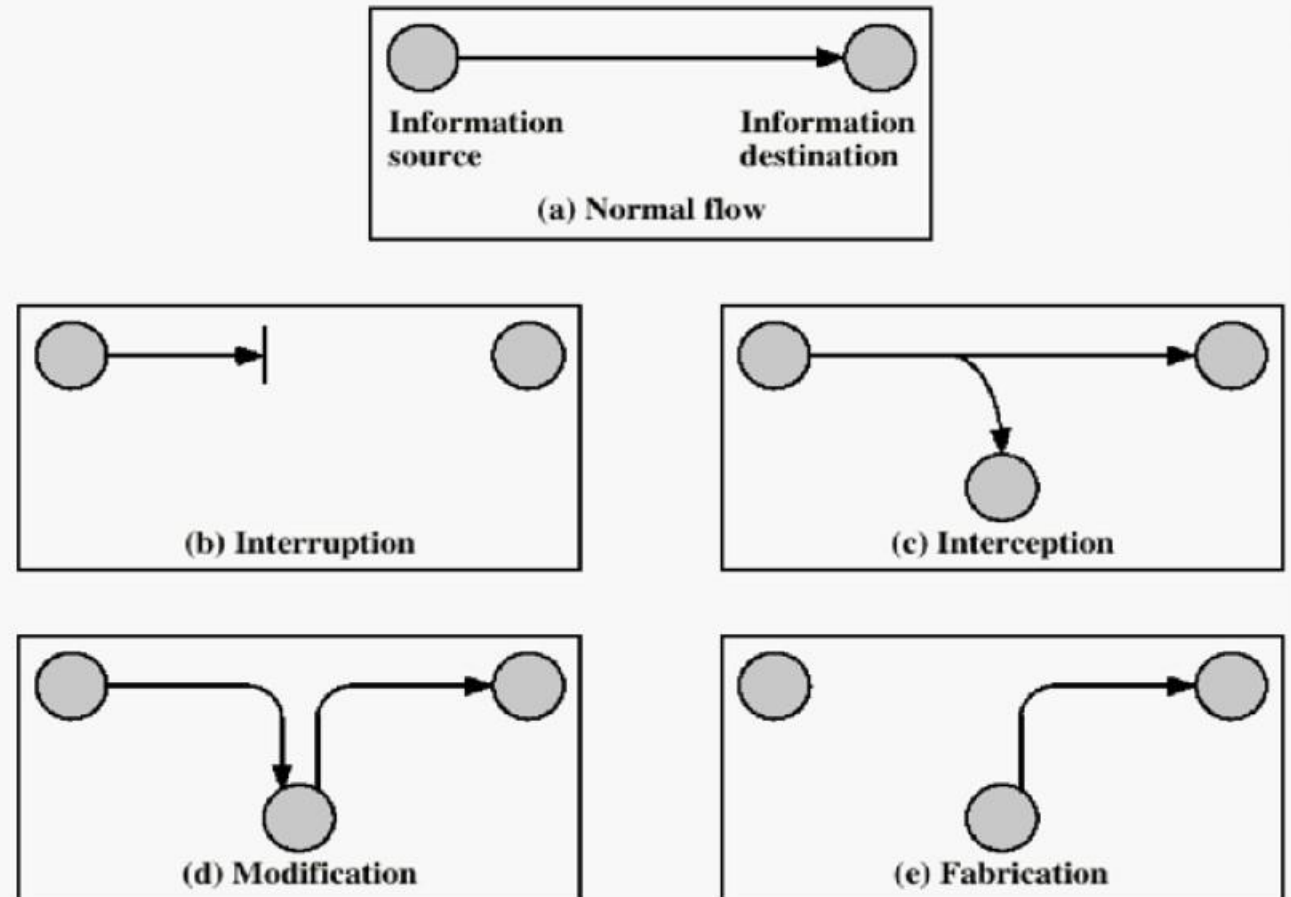


Figure 1.1 Security Threats

Type of Security Threat

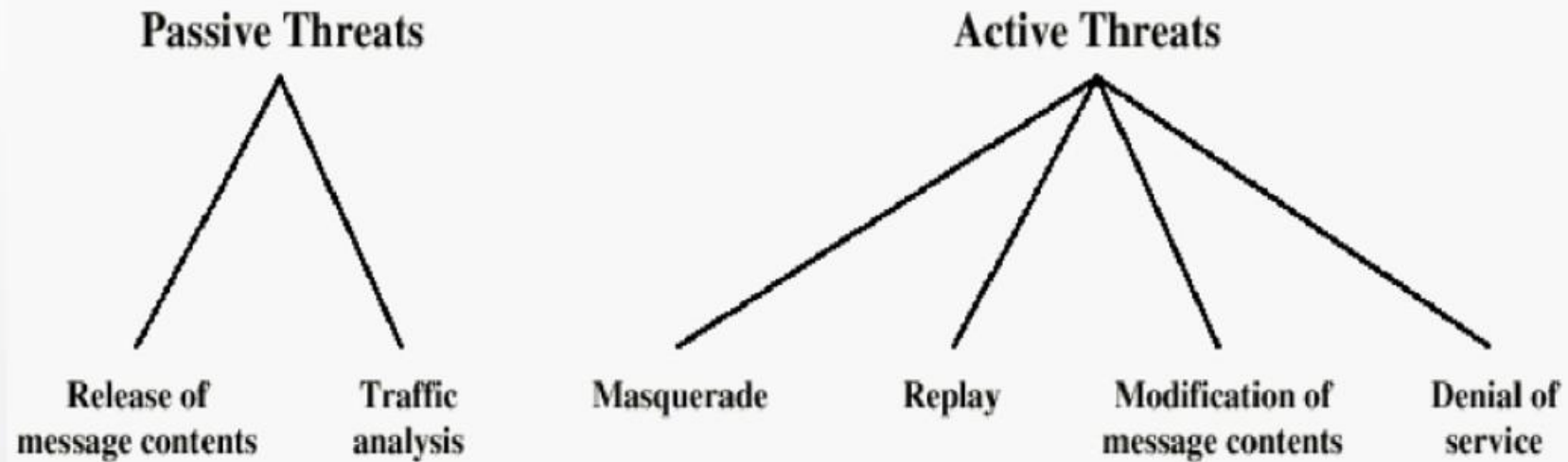
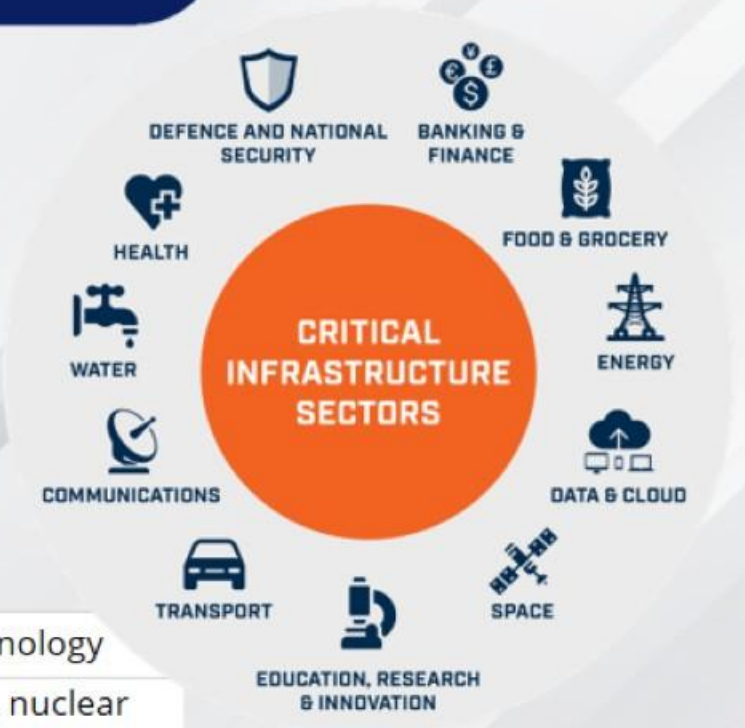


Figure 1.2 Active and Passive Security Threats

- Critical infrastructure describes the physical and cyber systems and assets that are so vital to the countries that their incapacity or destruction would have a debilitating impact on physical or economic security or public health or safety.

Critical infrastructure sector

Chemical	Dams	Financial services	Information technology
Commercial facilities	Defense industrial base	Food and agriculture	Nuclear reactors, nuclear materials, and waste
Communications	Emergency services	Government facilities	Transportation systems
Critical manufacturing	Energy	Health care, public health	Water and wastewater systems



- In the global environment with continuous network connectivity, the possibilities for cyberattacks can emanate from sources that are local, remote, domestic or foreign. They could be launched by an individual or a group. They could be casual probes from hackers using personal computers (PCs) in their homes, hand-held devices, or intense scans from criminal groups.

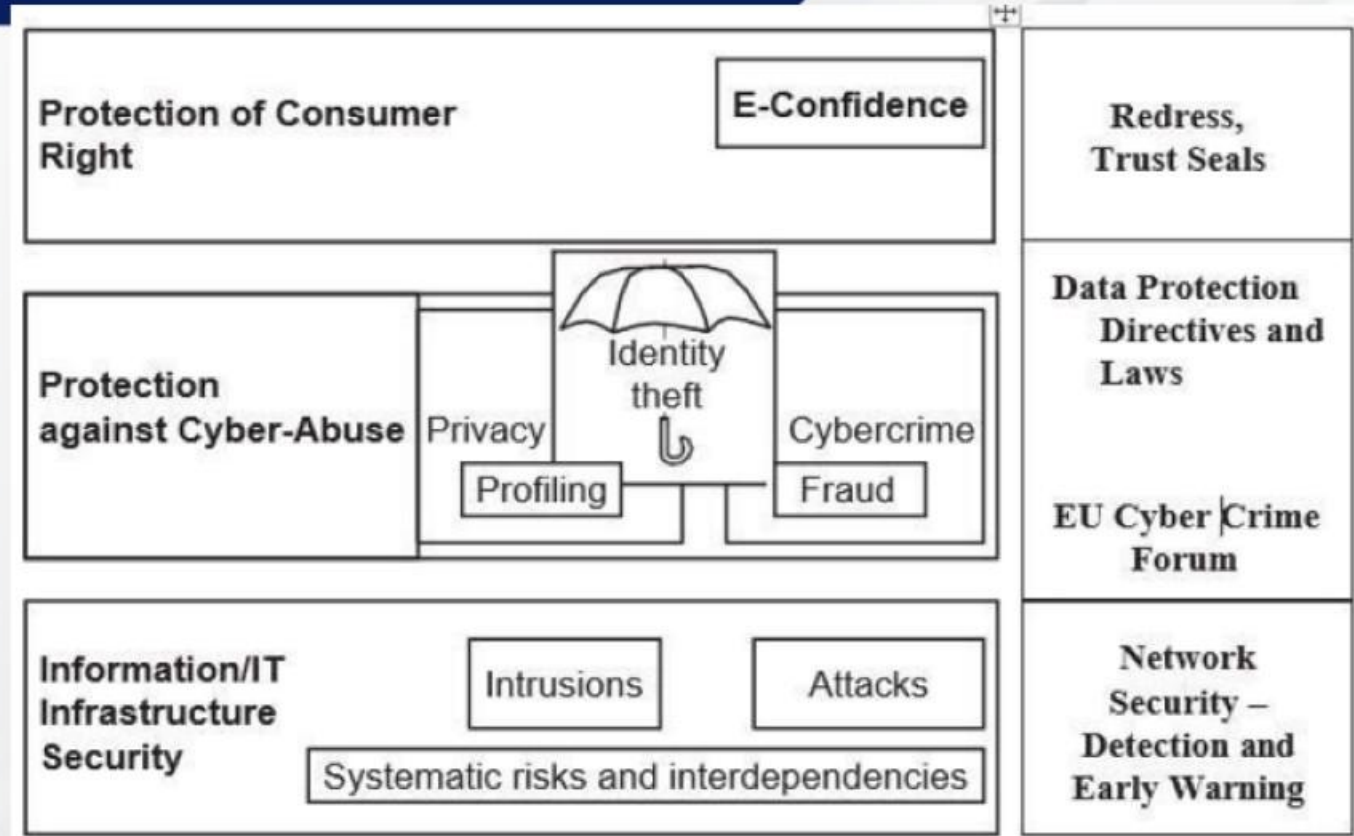


Fig: A cyber security perspective. EU is the European Union.

Cybercrimes cost a lot to organizations.

When a cybercrime incidence occurs, there are a number of internal costs associated with it for organizations and there are organizational impacts as well.

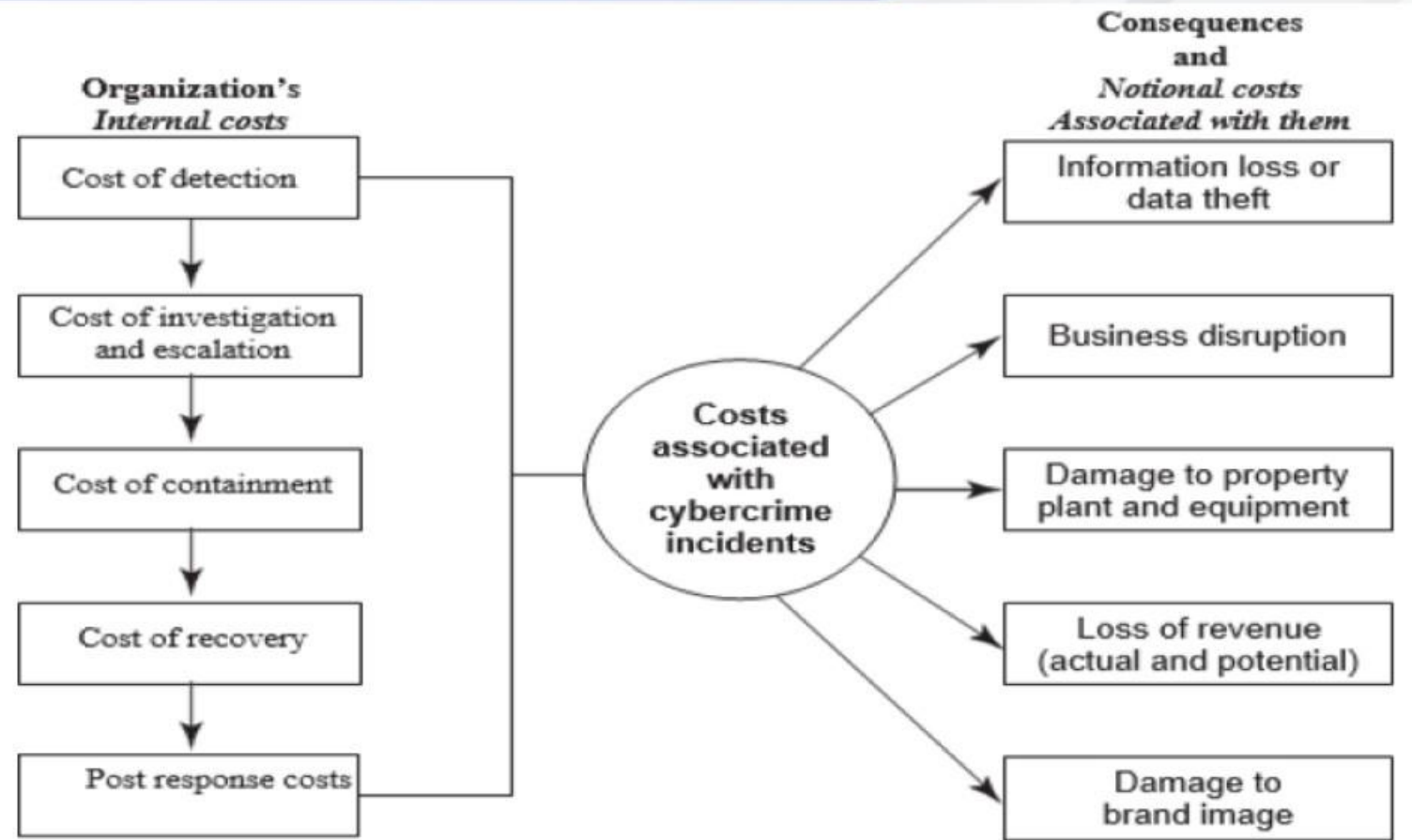


Fig: Cost of cybercrimes.

❖ Case Studies for:

- Biggest Cyber Threats in 2021. Case Study.
- Examples of Cyber Warfare Operations

The End 😊



Thank You