Types of Threats on Cyber Security System

Khalid Fadhil Jasim

Department of Computer Science
Cihan University-Erbil, KRG, Iraq
khalid.jassim@cihanuniversity.edu.iq

Outlines

- **Introduction**
- **Elements of Cyber Security**
- **Importance of Cyber Security**
- **Methods of Cyber Threats**
- **Conclusion**

Introduction

- Since the 1970s, computers have been used in various aspects commercially and personally.
- Despite their handiness, **computers** are also **prone** to **several threats.**
- **IBM and other early computer companies** have already **provided security software products** since the seventies.
- As the **computer and digital media development**, the **threats** also get **developed.**
- To counteract them, companies **nowadays** are **creating protection called Cyber Security.**

- **Cyber Security** refers to a **protection system for computers and networks from theft, damage,** disruption, illegal changing, or **information disclosure** taken from the electronic data, software, or hardware.

- The definition might seem simple, **but in reality,** the varied and enhanced **technologies like smartphones, websites**, **televisions**, **Internet of Things (IoT) require a complicated cyber security system.**

Elements of Cyber Security

- Based on the function and media, **cyber security system covers these types of security:**
  - **Data security:**

    In every single **network, hardware, and software,** there must be **data provided by the owners,** clients, or even the third party. **Data security** protects by giving **limited access only to the authorized** ones to prevent any data theft.
  - **Application security:**

    This type of security should be **developed from the design stage of the program. Continuous updates of the apps** should include the security system, so new **threats could be detected** early.
  - **Mobile security:**

    Mobiles including **tablets** and **cell phones** are also **prone to threats** that could **come from wire/devices** like USB and **wireless** like **Bluetooth and** the **internet.**

Elements of Cyber Security (Continued)

- **Endpoint security:**

  Users and entry points (users' **devices**) are most likely to **get malicious threats from a virus such as Malware.** The form of security could be anti-virus software, but the best one is the education for users to carefully plug in USBs, responding to suspicious links and more.

- **Cloud security:**

  Cloud is a digital data storage that enables users **to store and download data.** Although the **storage companies** also **run their cyber security system,** the **users also need** to be careful in **managing their cloud account** there have been many data thefts due to reckless Cloud account usage.

- **Database and Infrastructure security:**

  Not only the **digital software** but the **hardware** could **also be stolen. The security system** should **cover digitally and physically.**

Importance of Cyber Security

- **Cyber threats** could bring any **damages to the data, hardware/software,** and reputation. **Further problems** such as **data abuse and data leaking** are likely to happen.
- **All types of data and sensitive information must be protected.**
- **Stealing sensitive information and simple protections like anti-virus** app is **not enough to prevent the threats.**
- **Hence governments** participate in **making regulations related to cyber security.** An **example is General Data Protection Regulation** (GDPR) **in European Union.**

Types of Cyber Threats

- **Digital threats** are categorized into **three types:**
- **Cybercrime, Cyber-attack, and Cyber-terrorism.**
- **Cybercrime is organized by a person or a group** targeting **financial profit** or disruption.
- **Cyber-attack is mostly driven by political motives.**
- **Cyber terrorism is mostly done in massive act to cause certain fear.** To make those threats happen, cybercriminals usually use these methods. Some of these threats are given in the next slide.

Methods of Cyber Threats

- **Phishing:** the most frequent threat might be phishing. It is an **illegal act to steal** one's **private data** by **sending** them a **link that redirects to fake sites** or forms requiring users' personal information.
- **Malware:** acronym of **Malicious Software,** Malware enables **attackers or hackers** to have **access** to the **installed device.**
- **SQL Injection:** it stands for **Structured Query Language.** Just like its name, **SQL is a code injected** into an **entry field** that **exploits the security** vulnerability.

Methods of Cyber Threats (Continued)

- **Denial-of-service attack:** this attack employs ‘denial’ by the system by submitting the wrong password or overloading a network/machine’s capabilities to make the service unavailable. Another example is zombie computers.
- **Direct-access attack:** contrary to a denial-of-service attack, the direct-access attack is done by installing keyloggers, worms, a wireless mic, or covert listening devices to make operating system modifications for direct access to the original one.
- **Spoofing:** it is a masquerade act that comes from data falsification. Examples include biometric spoofing, IP address spoofing, and email spoofing.

Conclusions

- **Avoid any suspicious emails, chats, texts, or links from unknown senders.** Especially if they ask you to input your particular data.
- **Regularly update pins or passwords** with unique and strong ones. This could block access to the hackers that are currently logging into your account.
- **Never use public and unsecured Wi-Fi.** People could break into your device using a wireless connection.
- **Have a secure backup.**
- **Use cyber security technologies** such as **Identity and Access Management (IAM), Security information and event management (SIEM),** and data security platform.

Conclusions (Continued)

- Try **Third-Party Risk Management** (TRPM).
- **Employ IT professionals** that could detect any possible threats or protect from any hackers' attacks.
- **Choose cyber security strategy** at least choose some **software protection** like **anti-virus** or others.
- **Use multi-factor authentication** as it is harder to get broken down.
- **Do not recklessly log in** to various devices.
- Prepare for the worst by **making secondary plans in case** there is **data/resource loss.**

THANK YOU