

Name: JAY ARRE TALOSIG
Subject & Section: CTINASSL – COM231
Professor: Mr. Gaudencio Jeffrey G. Romano

Assignment #3: RISK

1. Discuss components of risk identification and give example.

Sa Risk Identification, basically dito natin inaalam kung ano ang pwedeng maging problema bago pa man ito mangyari. May three main components ito na usually magkakasama:

1. **Asset Identification:** Dito mo i-inventory lahat ng valuable assets ng organization. Hindi lang ito hardware, kasama din dito ang data, people, at procedures. Kung hindi mo alam na meron ka nito, hindi mo ito maprotektahan.
2. **Threat Identification:** Dito mo aalamin kung sino or ano ang pwedeng mag-cause ng harm. Pwede itong hackers, viruses, or kahit bagyo.
3. **Vulnerability Identification:** Ito yung mga weaknesses or butas sa system mo na pwedeng samantalahan ng threat.

Example Scenario: Imagine may Database ng Customer Credit Cards (Asset). Ang Threat ay isang Hacker na gustong nakawin ito. Ang Vulnerability ay hindi updated ang Windows Server mo (Outdated OS). Kapag nagsama-sama yan (Asset + Threat + Vulnerability), meron ka nang Risk.

2. Explain the attributes of hardware software and network assets to be tracked.

Kapag nag-iinventory or asset tracking, hindi pwedeng generic lang na "Laptop" or "Router" ang ililista. Kailangan detailed attributes para madaling ma-manage at ma-secure.

- **Hardware Attributes:** Dito tinitignan yung physical details. Importante to for tracking theft or maintenance.
 - *Examples:* Serial Number, Manufacturer/Model (e.g., Dell XPS 15), MAC Address (unique network ID), Location (kung nasan office or kung kaninong employee naka-assign).
- **Software Attributes:** Dito naman tinitignan yung programs na naka-install para ma-monitor ang licensing at updates.

- *Examples:* Software Name, Version Number (kritikal to para malaman kung kailangan ng patch), License Key/Serial Number, at Installation Date.
- **Network Attributes:** Ito yung details kung paano nagcoconnect yung devices sa network.
 - *Examples:* IP Address (static or dynamic), Subnet Mask, Gateway, at DNS settings.

3. Discuss the different kind of threats and give examples and explain.

Maraming categories ng threats, pero ito yung mga pinaka-common na kailangan mong bantayan:

1. **Human Error / Acts of Human Failure:** Ito yung mga aksidente lang at walang masamang intensyon. Usually employees ang cause nito.
 - *Example:* Isang employee na aksidenteng na-delete ang production database dahil akala niya test server lang gamit niya. Or nag-click sa phishing link kasi hindi niya alam na scam yun.
2. **Deliberate Software Attacks (Malware):** Ito yung mga program na sadyang ginawa para manira ng system.
 - *Example: Ransomware.* Ito yung ie-encrypt yung files ng kumpanya tapos hihingi ng bayad (bitcoin) para ma-unlock. Kasama din dito ang Viruses at Worms.
3. **Espionage or Trespass:** Ito yung unauthorized access para magnakaw ng information.
 - *Example:* Corporate spying kung saan yung competitor ay nagha-hire ng hacker para nakawin yung confidential "secret recipe" or blueprints ng kumpanya niyo.
4. **Forces of Nature (Acts of God):** Mga threats na hindi tao ang may gawa, kundi kalikasan.
 - *Example:* Baha, sunog, or lindol na pwedeng sumira sa server room. Kaya importante ang off-site backups.
5. **Technical Hardware Failures:** Pagkasira ng equipment dahil sa luma na or defects.
 - *Example:* Hard drive crash sa server kung saan nandoon lahat ng files, or power supply failure.

4. What are the risk control strategies? Explain each.

Kapag na-identify mo na ang risks, kailangan mo ng strategy kung paano ito haharapin. Ito ang limang common strategies:

1. **Defend (Avoidance):** Ito yung priority strategy. Gagawin mo ang lahat para *hind* mangyari yung risk. Naglalagay ka ng safeguards.
 - *Explanation:* Mag-iinstall ka ng firewall, antivirus, at magtuturo sa employees para hindi sila ma-hack. "Prevention is better than cure" ang peg nito.
2. **Transfer (Transference):** Iilipat mo yung risk sa ibang party para hindi ikaw ang sasalo ng buong impact kung mangyari man.
 - *Explanation:* Pagbili ng **Cyber Insurance**. Pag na-hack kayo, insurance company ang magbabayad ng damages. Pwede ring pag-outsource ng security sa ibang company (MSSP).
3. **Mitigate (Mitigation):** Tanggap mo na pwedeng mangyari yung risk, pero gagawa ka ng paraan para bawasan ang damage.
 - *Explanation:* Incident Response Plan at Backups. Kung ma-ransomware man kayo (nangyari na), may backups kayo para ma-restore agad ang data at hindi masyadong malaki ang lugui.
4. **Accept (Acceptance):** Wala kang gagawin. Tanggap mo na yung risk kasi mas mahal pa ang solusyon kaysa sa halaga ng asset na pinoprotektahan.
 - *Explanation:* Kunwari may lumang printer na walang security feature. Mas mahal pa bumili ng firewall para dun kaysa bumili ng bago pag nasira, so hahayaan mo na lang (Risk Appetite).
5. **Terminate:** Ititigil mo na mismo yung activity or process na nagdudulot ng risk.
 - *Explanation:* Kung masyadong risky ang paggamit ng lumang Windows XP sa network niyo, tatanggalin na lang totally ang Windows XP computers. Wala nang asset, wala nang risk.

5. References

- Whitman, M. E., & Mattord, H. J. (2021). *Principles of Information Security* (7th ed.). Cengage Learning. (Most concepts like Risk Control Strategies and Threat Categories are based on this standard textbook).

- **NIST Special Publication 800-30 Rev. 1. *Guide for Conducting Risk Assessments*.** National Institute of Standards and Technology. (Standard for Risk Identification components).
- **Stallings, W., & Brown, L. (2018). *Computer Security: Principles and Practice* (4th ed.). Pearson.**