

By Kemal J Abdullah

Cybersecurity*

** From "not so consultant" POV*

Surabaya, 01 November 2024

Profile



Background:

- Bachelor's degree in Computer Science, Information System, Ten Nopember Institute of Technology (ITS). Graduate in 2021
- Associate IT Risk Advisory – Deloitte Konsultan Indonesia (2021 – 2024)
- ▶ Senior Technology Consultant – Cybersecurity at EY Indonesia with a focus on cybersecurity GRC
- ▶ Kemal has deep experience in **IT Governance, Risk and Compliance (GRC)** before joining the EY Cyber Technology Consultant team

Skills:

- ▶ *Cybersecurity*
- ▶ *Information Security*
- ▶ *IT Audit*
- ▶ *IT Governance, Risk and Compliance (GRC)*

Relevant experiences and clients:

- ▶ Perform **IT Audit** for several major Indonesia's company in financial service, oil and gas, mining, manufacturing, and retail industries.
- ▶ Perform **application control review** as part of financial audit for several major Indonesia's financial services and **telecommunications company**.
- ▶ Conducted **IT security governance** upgrade projects for several state-owned companies engaged in energy and investment
- ▶ Perform Internal Control Over Financial Reporting (ICFR) implementation project regarding application control in one of the biggest oil company in Indonesia.
- ▶ Perform Internal Control Over Financial Reporting (ICFR) implementation project regarding application control in state own company
- ▶ Act as consultant for internal auditor regarding SOX implementation in one of the biggest bank in Indonesia.

Opening....

Do you know, how much cyber attack that targeting Indonesia in 2023 based on data that has been released by BSSN (Badan Siber dan Sandi Negara)??

403 Million

That's why we need to tightened up our **Cybersecurity** capabilities...

Wait, what is...

Cybersecurity?

Cybersecurity refers to the practice of protecting systems, networks, and programs from **digital attacks**.

Cybersecurity measures are essential for protecting data, maintaining privacy, and ensuring the reliability and safety of digital systems.

Source: EYQ Glossary

And what is the core of Cybersecurity???

People

&

Technology

These two things must go hand in hand and cannot walk alone, why?? Pay attention to next slide

Example of Digital Attack (Cyber Attack)

- Phishing
- Man in the Middle
- Malware
- Ransomware
- Cross Site Scripting
- DoS and DDoS attack
- SQL Injection
- Brute Force
- Social Engineering
- Credential Stuffing
- Insider Threat

Okay, now how do we know that the security of a system in a company or organization is reliable??

First, Attack

We will conduct **Vulnerability Assessment** and/or **Penetration Testing** to evaluate the gaps.

Secondly, Audit

We will assess all the process related to IT environment to ensure the **risk has been addressed** by management (**people**) and the daily operations are conducted based on applicable **standard and procedure**.

Ok, now we talk about how company protect themselves from cyber attack?

Technical Measures

1. Firewall and Intrusion Detection System (IDS)
2. Encryption
3. Patch Management
4. Anti Virus
5. Multi Factor Authentication (MFA)
6. Network Segmentation
7. Backup and Recovery

Non - Technical Measures

1. Security Policy and Procedures
2. Employee Training and Awareness
3. Incident Response Plan
4. Vendor and Third-Party Risk Management
5. Regular Audit
6. Compliance with Regulations

QUIZ!!

Is that okay, if one of the measurement to prevent the cyber attack is not implemented by related company or organization??

That's it, any question?