Topic 7

Data Protection Fundamentals

Slides developed by

What you will learn in these slides...

- Importance of data protection
- Data protection-related legislations
  - DPP, PDPA, GDPR
- Data Loss Prevention (DLP)
- Documents and terms used in data protection
  - Frameworks and standards
  - Encryption, Backup, Retention, Erasure

Recap on Topic 1

- CIA Triad
- AAA Model
- Asset, Vulnerability, Risk, Threat
  - In Topic 1, we learnt that assets can be either physical or digital
  - For this topic, the term ‘Data’ will mainly refer to digital assets

Why do we need to protect our data?

- Maintaining CIA and adhering to AAA
  - Ensure that sensitive data
    - C: Remains confidential
    - I: Is not tampered with
    - A: Is available to authorized users
  - Regular auditing is vital in ensuring that proper data protection procedures are followed
    - The third A in AAA stands for Accounting, which is similar to Auditing (may be used interchangeably)
- Build trust among people
  - In businesses, protecting customer data is important
  - Some data protection practices are required by law, and following them upholds an organization's reputation and ensures legal compliance

Data protection-related legislations

- Data Protection Policy (DPP)
  - Implemented by most organizations. It outlines the guidelines and procedures for handling personal and sensitive data within an organization.
  - Aims to safeguard the CIA of data
- Personal Data Protection Act (PDPA)
  - Provides a baseline standard for personal data protection in Singapore
  - Comprises 11 obligations
- General Data Protection Regulation (GDPR)
  - Controls how personal data of people in the European Union (EU) is processed and transferred

Reference: https://www.pdpc.gov.sg/overview-of-pdpa/the-legislation/personal-data-protection-act, https://www.consilium.europa.eu/en/policies/data-protection/data-protection-regulation/

Data Loss Prevention (DLP)

- A set of strategies, tools, and processes used to ensure that sensitive data is not lost or tampered with by attackers

Importance in cybersecurity

- Prevents unauthorized access to any kinds of data
- Helps organizations comply with data protection laws and regulations, like GDPR
- Mitigates the risk of data breaches, which could lead to financial loss, legal penalties, and reputation damage

Some key components of DLP

- Endpoint protection
  - Endpoint devices include desktops, laptops and tablets to name a few. Implementing DLP on these devices helps to prevent data breaches.
- Incident response (IR)
  - A good use of DLP is to develop an incident response plan for data breaches. This will help define the procedures organizations should follow in case of such events. (We will go more in-depth on IR in Topic 8)
- Classifying data based on sensitivity level
  - Identify and classify sensitive data based on pre-defined categories
    - Some examples include personal data, financial records, or intellectual property

Frameworks and Standards

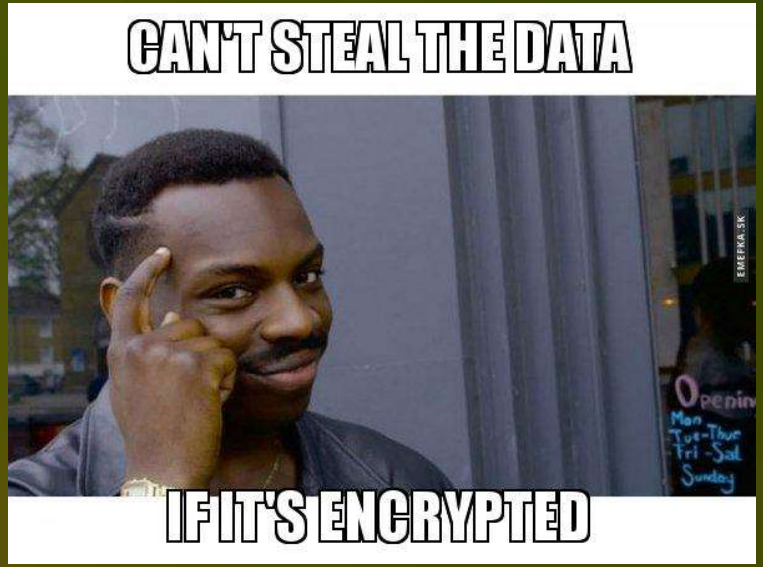
- They provide structured approaches and guidelines to help organizations manage cybersecurity risks
- Ensure an organization's compliance with regulatory requirements

Some differences between frameworks and standards

Framework	Standard
• Includes strategic approaches and methodologies • Covers multiple areas of cybersecurity • Guidelines are voluntary and more flexible/adaptable to various organizational needs • Examples include: NIST Cybersecurity Framework, COBIT 5	• Includes specific, measurable guidelines and criteria • Focuses on specific areas of cybersecurity • More rigid with specific requirements that must be met • Examples include: NIST SP 800-53, ISO/IEC 27001 (the most well-known standard for information security management systems (ISMS))

Common terms/actions in data protection

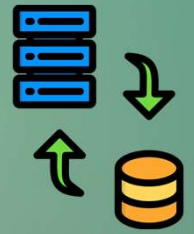
- Encryption
- Backup
- Retention
- Erasure



Data Encryption

- A method that turns readable information into what looks like gibberish
- Can only be decrypted with a key or password (similar to the accounts you own)
- This makes it tougher for hackers to decipher the message
- Popular encryption algorithms include
  - AES (Advanced Encryption Standard)
  - RSA (Rivest, Shamir, Adleman, the inventors of this algorithm)
  - Twofish

Data Backup



- Making copies of your original work to ensure that you still have a copy if the original goes missing
- Backups are best stored in safe places

Some good practices for Data Backup

- Store backups in an external hard drive or a USB flash drive
- Use cloud storage services to store your files on encrypted remote servers, only requires an Internet connection to access them
  - Examples include Google Drive, iCloud, Dropbox etc.

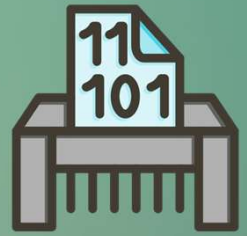
Data Retention

- Various ways that an organization manages how long data is kept and maintained
- Often stated and defined in an organization's policies
- Ensures sensitive information is not kept longer than necessary, reducing the risk of data breaches

Some good practices for Data Retention

- Categorize data based on sensitivity, importance, and required retention period
- Conduct regular audits to ensure compliance with retention policies

Data Erasure



- Usually occurs after the data retention period
- Securely removes data from devices to ensure they cannot be recovered by hackers
- Involves overwriting the data multiple times to ensure it is permanently destroyed
  - This is different from normal file deletion, which only removes the reference to the data and leaves the actual data intact until overwritten

Data Erasure Methods

- Policy Implementation
  - Implement a data erasure policy that outlines the proper procedures. Ensure the policy is enforced and acknowledged across all departments
- Multiple overrides
  - Implement overriding methods, where data is overwritten multiple times to ensure sensitive data is fully erased before destruction
- Physical destruction
  - After erasing data, destroy the storage device (usually by degaussing or shredding for hardcopy documents)
- Conduct regular audits (often done after the erasure process)
  - To confirm that all targeted data has been completely and irreversibly erased
  - Helps to identify and address any gaps or weaknesses in the erasure process

Topic 7 Summary

- Importance of data protection
- Data protection-related legislations
- Data Loss Prevention (DLP)
- Actions to take for data protection

In the next and final topic (you're almost there)...

Incident Response Fundamentals

- NIST Incident Response Life Cycle
- Response plans used in organizations