Lesson 3

Data Security Policy

ST2610

Security Policy & Incident Management (SPIM)

Growth of Computer Networks & the Internet – Huge Impact on Society

- Over the last 3 decades, computer networks have made pervasive inroads in our everyday lives, both in **business** as well as at **home**
- The Internet came along and connected the world
- Computer networks enable efficient **collection**, **manipulation** and **storage** of data – and vast quantities of it too
- **Data can be stored anywhere in the world**
  - Not necessarily where it is collected
- Gigabytes of **personal data** are accessed and used on a daily basis
- New threats affecting privacy and data protection e.g. identity theft, etc.

Key Consideration for Cybersecurity – Assets

- Data
  - Business Data
    - Business & Operations Plans
    - Financial Information
    - Transactions
    - Communications
    - Logistical Information
    - Manufacturing & Inventory Information
    - Archives & Records
    - Intellectual Properties e.g. Patents
    - Research & Discoveries
    - Other Trade Secrets
  - Personal Data
  - Public Data, etc.
- Systems including Infrastructure and Network
- Services

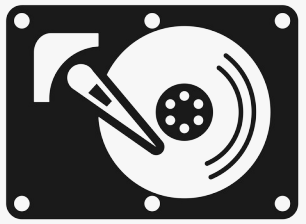
Data Types

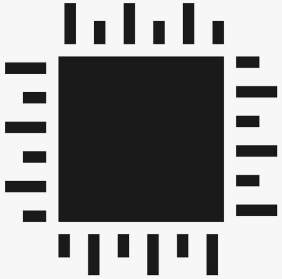
- Official v. Personal
- Commercial v. Social
- Internal v. External
- Admin v. Business

"If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle."
Sun Tzu, The Art of War

States of Data

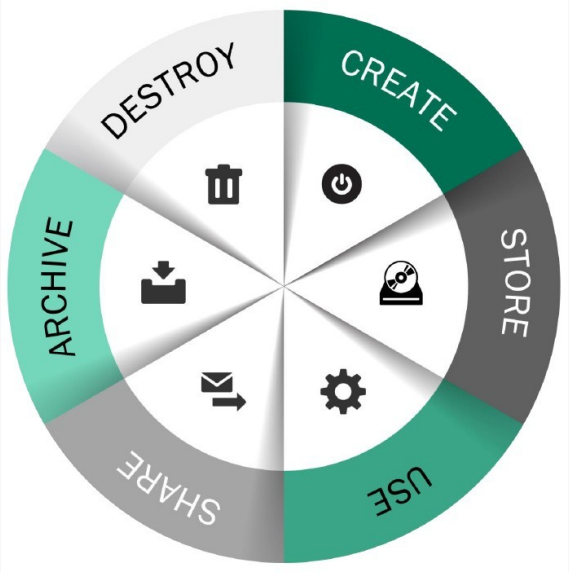
- Data at Rest
- Data in Motion
- Data in Use





Class Activity Discuss how do you secure each data state. At which state is the most difficult to protect the data?

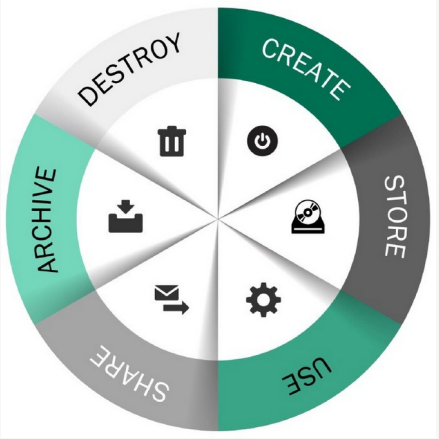
Data Life Cycle
& Key Data Functions



	Create	Store	Use	Share	Archive	Destroy
Access	X	X	X	X	X	X
Process	X		X			
Store		X			X	

Class Activity **Match the Description**

a. Create
b. Store
c. Use
d. Share
e. Archive
f. Destroy

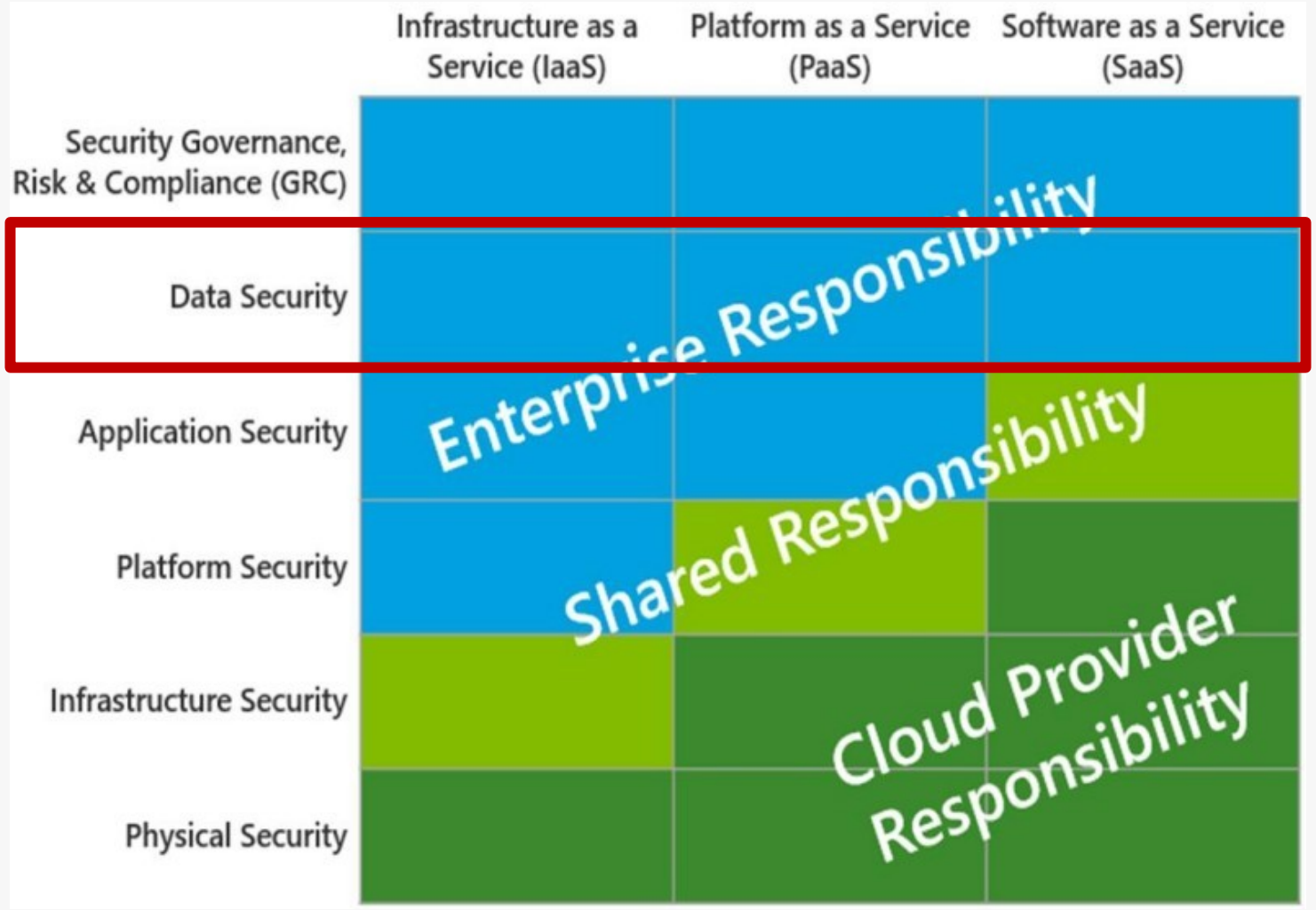


- Making information accessible to others
- Generation of new content
- Viewing or processing of data
- Data enters long-term storage
- Typically occurs at the same time as creation
- The end of the lifecycle

Data Security Considerations

- At what stages in each **life cycle** can data move between locations?
- **How does data move** between locations?
- What is/are the **potential location(s) for data** I have to protect?
- **Who are the actors** that potentially have access to the data I need to protect?
- **Where are these actors** coming from?
- **What are the controls** in each of those locations?

Data Security Responsibility / Accountability



– To be revisited in Lesson 05: Cloud Security Policy

Components of Data Security

- Data Labelling
  - Unclassified, Restricted, Confidential, Secret, Top Secret …
- Data Handling
- Data Processing
- Data Security / Protection

Cybersecurity Threats to Data

- Unauthorised Access
- Unauthorised Usage
- Theft or Accidental Loss of Storage Media
- Data Leakage / Breaches
- Unauthorised Modification / Corruption / Destruction of Data
- (Distributed)-Denial-of-Service (DoS/DDoS)
- Malware
- Improper Treatment or Sanitisation After End-of-Use

Basic Data Protection Mechanisms

- Securing the Electronic Devices & Applications e.g. Hardening
- Encryption
- Authentication e.g. Password, 2FA
- Access Control e.g. Principle of Least Privilege, Segregation of Duties, etc.
- Physical Protection
  - Network Segmentation
  - Defence-In-Depth (Multi-Layer)
  - Physical Locking & Storage
  - Disconnect from Internet / LAN

Data Security Solutions & Controls

some e.g.

- Encryption
- File & Database Access Monitoring
- Data Leakage Prevention (DLP)
- Data Sanitisation
  - Anonymisation
  - Obfuscation
  - Tokenisation
  - Masking

"Names has been changed to protect …" ABC123 = A1B2C3Z1Y2X2

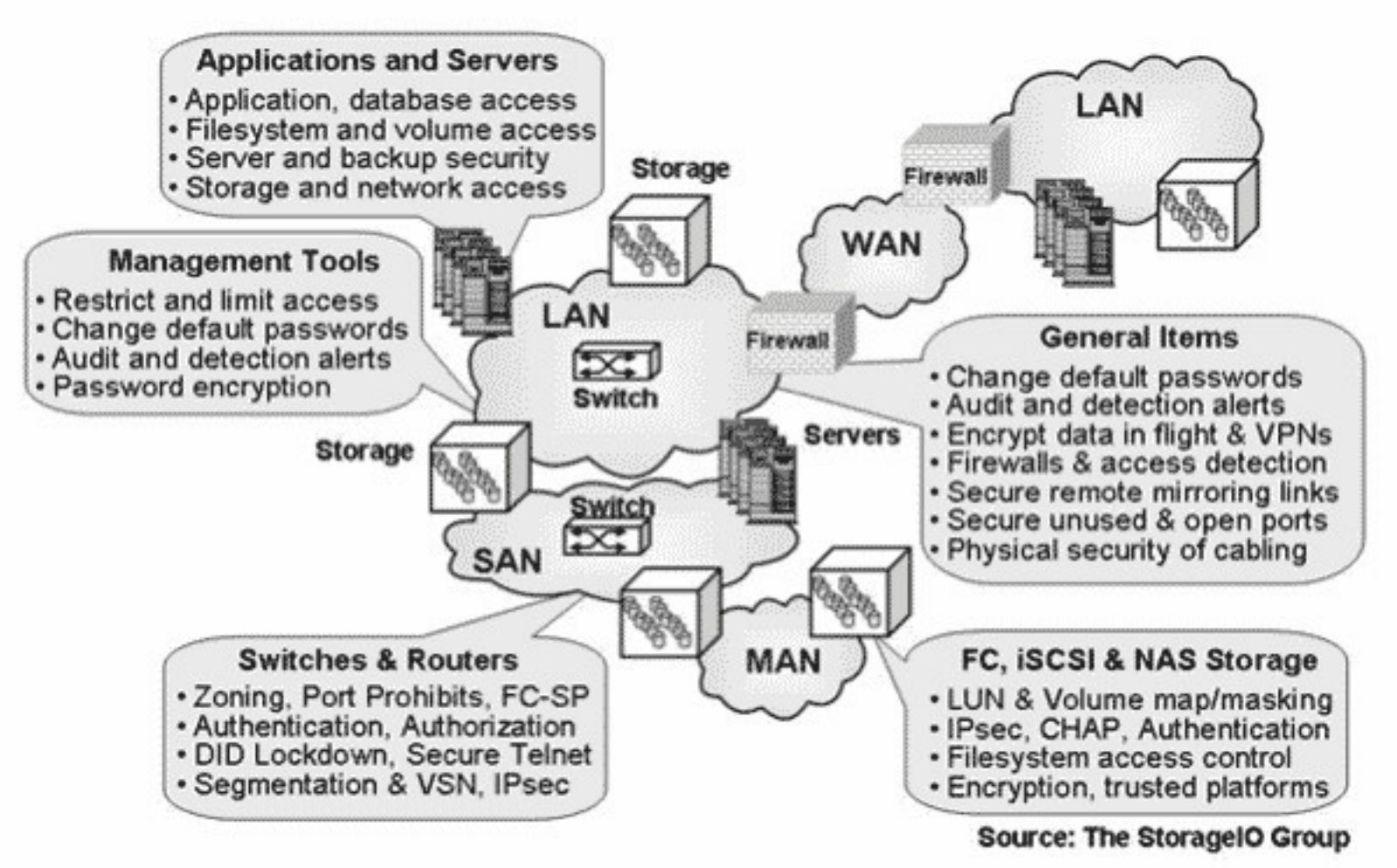
Use of a "nickname" which itself has no value 4539-XXXX-XXXX-2205

Secure Deletion of Data

- Low-Level Deletion / Formatting
- Degaussing
- Physical Destruction
- Crypto-Shredding e.g. 1-Way Encryption

Data Protection in the IT Infrastructure | an

e.g.

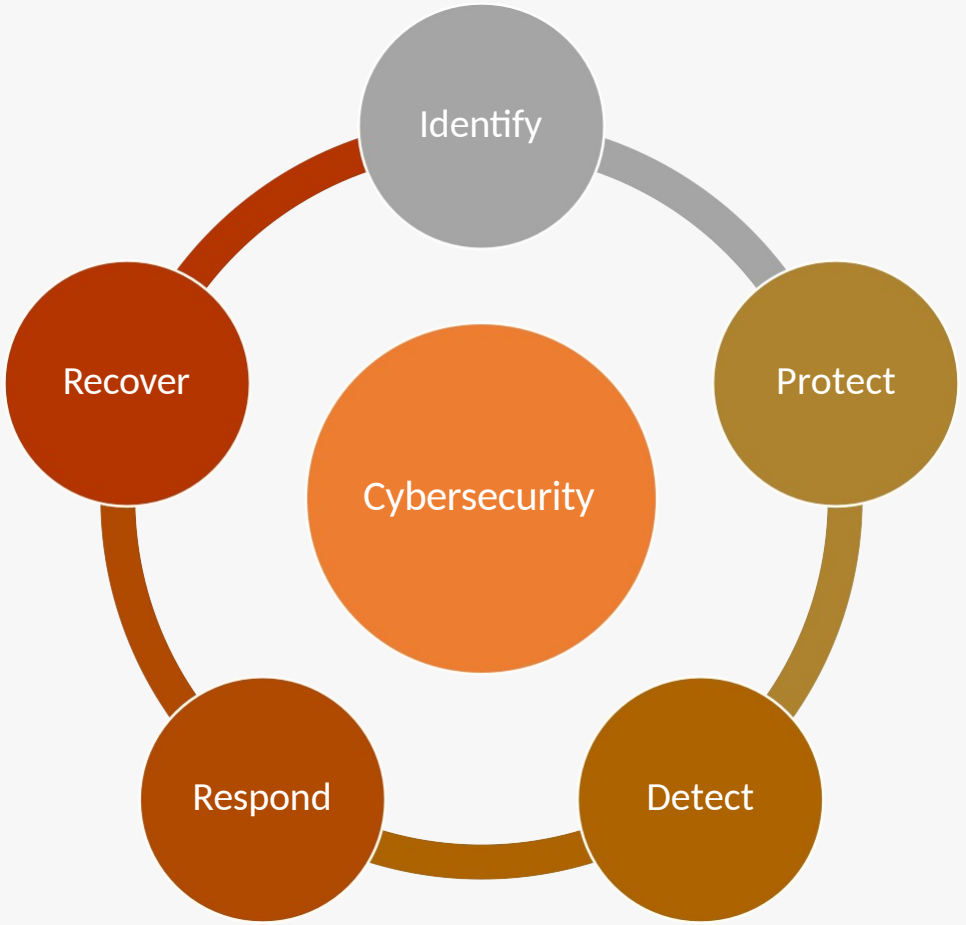


Challenges & Recommendations

- Business Challenges
  - Expensive
  - Need more resources to manage e.g. Security Administrator(s)
  - Need additional hardware/software and processing capabilities
- Solution Challenges
  - Legacy Application Changes
  - Application Integration
  - Performance Issues
  - Key Management for Encryption

- Recommendations
  - Trade-off between Security & Performance
  - Apply appropriate security strategy keeping performance and data flow in mind
  - Separation of Environment

5 Core Cybersecurity Functions



– Remember your Detection, Response & Recovery Capabilities as well

Personal Data Protection

- Very important in current societal context
- Legislations & Regulations
  - Personal Data Protection Act (PDPA) | Singapore
  - General Data Protection Regulation (GDPR) | European Union (EU)

– Note: Privacy v. Personal Data Protection

Personal Data Protection | The Problem

- Huge amount of data about you can be stored on computer, and easily searched.
  - Data can be lost, stolen, or transferred to another country easily.
- People need protection from careless or inaccurate processing of data about them, they also need to be able to see what data is being held about them.

Personal Data

- Personally Identifiable Information (PII)
  - NIST: Any information about an individual, including:
    - (1) Any information that can be used to distinguished or trace an individual's identity
      e.g. name, social security no. date and place of birth, mother's maiden name, or biometric records; and
    - (2) Any information that is linked or linkable to an individual
      e.g. medical, educational, financial, and employment information.
  - Absence of PII does not mean that the remaining data does not identify individuals
- Personal Data (PD)
  - GDPR: Any information relating to an identified or identifiable natural person;
    - An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier e.g. name, an identification no., location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identify of that natural person.
  - PDPA: Data, whether true or not, about an individual who can be identified –
    - (a) from that data; or ….
- Quasi-/Pseudo-Identifiers
  - PII? No
  - PD? Yes

PDPA | Singapore

- Ensure that organisations take care of personal data understand their possession or in their control
- Restrictions on Collection / Use of Personal Data
- 2 Components
  - Do Not Call (DNC) – Re: Privacy
  - Personal Data Protection
- Data Management

Personal Data Protection through Management & Governance

- Appoint a DPO
- Review the Personal Data Inventory
- Ensure Cybersecurity / Personal Data Protection Policies, Standards, Guidelines and Procedures
- Communicate Internally
- Establish an Internal Audit Policy

External Auditor v. PDPA

Data Intermediaries Obligations

- "If the external auditor is processing Personal Data on behalf of and for the purposes of the company, and this is done pursuant to a contract which is evidenced or made in writing, then the external auditor may be a Data Intermediary (DI) for the purposes of the PDPA that can benefit from the partial exclusion under §4(2) i.e. subject to fewer Data Protection obligations."
- PDPA 2012
  - §2(1) Interpretation
    - "Data Intermediary" means an organisation which processes personal data on behalf of another organisation but does not include an employee of that other organisation.
  - §4(2) Application of Act
    - Part III to VI (expect for §24 (protection of personal data) and §25 (retention of personal data) shall not impose any obligation on a data intermediary in respect of its processing of personal data on behalf of and for the purposes of another organisation pursuant of a contract which is evidenced or made in writing.
  - Part III – General Rules with Respect to Protection of Personal Data
  - Part IV – Collection, Use and Disclosure of Personal Data
  - Part V – Access to and Correction of Personal Data
  - Part VI – Care of Personal Data

PDPA | The Significance

- Concept is not new, but only recently made official, starting with EU's Data Privacy Laws
- A State Law, hence punishable
- Implemented by many countries
- Increase responsibility for personal data protection
- Increase overall cybersecurity awareness and practices

Cybersecurity Threats to Electronic Personal Data

- Hacking or other unauthorised access of databases
- Physical attacks e.g. use of skimming devices on ATM
- Malware or hostile programs e.g. computer viruses and spyware
- Social Engineering e.g. phishing scams and the circulation of malware-laden email attachments
- Unauthorised access or misuse of personal data by employees or vendors
- Loss or theft of electronic devices or portable storage devices containing personal data
- Fault or weakness in a system's or device's program code causing it to reveal personal data to incorrect parties e.g. a bug in an online portal allowing someone to access another person's data
- Compromised network devices
- Compromised POS systems
- Not disposing of electronic personal data properly
- Unintended disclosure of personal data to another individual other than the intended recipient e.g. emailing to the wrong recipient

PDPA | The 9 Main Data Protection Obligations

1. Consent
2. Purpose Limitation
3. Notification
4. Access & Correction
5. Accuracy
6. Protection
7. Retention Limitation
8. Transfer Limitation
9. Openness

Sensitive/Special Personal Data | GDPR

- Racial or Ethnic Origin
- Political Opinions
- Religious or Philosophical Beliefs
- Trade-Union Membership
- Health, Sex Life or Sexual Orientation
- Genetic Data
- Biometric Data (where this is used for identification purposes)

Personal Data Protection Guidelines

- Advisory in nature and do not constitute legal advice
- Provide guidance on the manner in which the Commission will interpret provisions of the PDPA
- Types of Guidelines
  - Main Advisory Guidelines
  - Sector-Specific Advisory Guidelines
  - Industry-Led Guidelines
  - Others

e.g. PDPC Published General Guides

- Guide to Securing Personal Data in Electronic Medium
- Guide to Managing Data Breaches
- Guide on Building Websites for SMEs
- Guide to Developing a Data Protection Management Programme
- Guide to Data Protection Impact Assessments
- Guide to Basic Data Anonymisation Techniques

https://www.pdpc.gov.sg/Legislation-and-Guidelines/Guidelines

Territorial Scope of Data Protection Law & Transborder Data Flow

"I wake up every morning deciding which country's law am I going to break today."
– A MNC CISO