Data Protection, Ethics & Social Issues

definitions are highlighted!

Importance of privacy and integrity of data

- Protect sensitive personal information and preserve confidentiality
- Mitigate risks
- Ensure compliance with regulations
- Build trust

Ways to protect data

- Access control
    - Strict access control measures ensure that only authorised individuals can access sensitive data
    - e.g. Strong passwords, two-factor authentication, role-based access controls
- Encryption
    - Encrypting data at rest and in transit preserves its confidentiality if it is stolen or lost
    - Converts data into an unreadable format; only authorised parties with the encryption key can decrypt and access it
    - e.g. Strong encryption algorithms, secure key management practices
- Regular backups
    - Regularly backing up important data ensures that it can be restored in the case of accidental deletion, data corruption or system failure
    - e.g. Secure backup storage (off-site to protect against physical disasters)
- Physical security

    - Prevents unauthorised access, theft or damage to servers and devices
    - e.g. Restricted access to server rooms, surveillance systems, secure storage for backup media
- Firewalls and intrusion detection systems (IDSs)
    - Deploying these prevents and detects unauthorised network access.
    - Firewalls restrict incoming and outgoing traffic based on security rules.
    - An IDS monitors network activity and alerts administrators to suspicious or unauthorised access attempts.
- Secure software development
    - i.e. Following secure coding practices when developing software/applications that handle sensitive data
    - e.g. Input validation, output encoding, protection against common vulnerabilities (like SQL injections)
- Security awareness training
    - Educating students and staff about the best data security practices reduces human error.
    - e.g. Teaching them about the importance of strong passwords, avoiding phishing attempts, being cautious with personal data
- Patch management
    - Keeping software and systems up to date with the latest security patches and updates addresses vulnerabilities and exploits, which could otherwise be used to gain unauthorised access to data.
- Data minimisation
    - Only collecting and retaining the minimum amount of data necessary reduces the risk of data exposure in case of a security breach.
- Incident Response Plan

    - Such a plan defines response and recovery procedures, helping to rapidly contain breaches, limit damage and restore systems quickly.

Backups and archives

- *Backup — a duplicate of active data that can be quickly restored in case of accidental deletion, corruption or system failure*
    - Safeguards against hardware failures, cyberattacks and national disasters — allows for resumption of operations with minimal disruption
- *Archiving — storing a copy of old and unused data for long-term retention*
    - Usually on cost-effective storage media (e.g. optical disks, compressed formats)
    - Frees up space on primary systems
    - Ensures access to historical data for auditing, legal compliance and reference purposes
- Both should be stored in offsite locations or cloud platforms to provide protection against physical damage, theft or localised incidents.
- Multiple backups and further distribution of archives enhances data resilience by implementing redundancy.
- Backup and archiving strategies should align with organisational data retention policies, which define:
    - How long data should be kept
    - Frequency of backups/archiving
    - Criteria for secure deletion

Version control

- *A system for managing changes to files, documents or datasets over time*
- **Accountability:** Maintains a comprehensive history of changes, providing an audit trail that allows tracking and reviewing of modifications
- **Collaboration:** Allows multiple individuals to work concurrently, merge changes and resolve conflicts
- Maintains content integrity
- Allows us to roll back to previous versions, supporting iterative development — allows continuous refinement and improvement of files or projects without losing previous work

Naming convention

- Standardized rules for naming files, folders, variables, functions, classes and other resources
- Consistent and meaningful names improve readability, organisation, maintainability, and make it easier to understand the purpose of a resource at a glance
- Allows for easy navigation of resources
- Maintains clarity across systems
- e.g. **In programming:** camelCase for variables and methods, PascalCase for class names
- e.g. File management, project documentation, websites, collaborative resources

Personal Data Protection Act (PDPA)

- A data protection law to regulation how organisations collect, use and disclose personal data

- Addresses the ethical concerns related to privacy, consent and data security that arise from the collection, storage and use of personal data
- Ensures organisations are accountable for their data handling practices and allows individuals control over their personal information
- Balances technological development with protecting individuals' privacy rights
- Under the PDPA, organisations must appoint a Data Protection Officer (DPO) to oversee compliance; the DPO ensures that PDPA requirements are met, promotes data protection awareness, manages data-related complaints, identifies risks, and liaises with the Personal Data Protection Commission (PDPC) when necessary.
- 4 key obligations:
    - **#1: Consent** — organisations must obtain clear and informed consent before collecting, using or disclosing personal data.
    - **#2: Purpose limitation** — personal data must only be collected for specific and reasonable purposes.
    - **#3: Protection** — organisations must implement security measures to prevent unauthorised access, disclosure or data loss.
    - **#4: Retention limitation** — personal data should not be kept longer than necessary.
- Failure to comply with the PDPA may result in investigations, financial penalties, reputational damage, legal consequences and business disruption.

Code of ethics of a Computing professional

- Ethics in computing refers to professional rules of conduct guiding moral behaviour.

- A code of ethics maintains high ethical standards, promotes trust and integrity in the profession and ensures that public interest is central to professional decisions.
- Professional bodies like the Association for Computing Machinery (ACM) and the Institute of Electrical and Electronics Engineers (IEEE) have **global** influence; their codes of ethics provide guidance and standards for professional conduct in the computing and technology fields, and promote ethical and responsible behaviour.
- The Singapore Computer Society (SCS) provides a Code of Ethics and Conduct for IT professionals in **Singapore**.

	Areas of conduct	Examples
1	Integrity and honesty	Act ethically and truthfully, avoid conflicts of interest, do not overstate competence
2	Responsible use of technology	Use technology ethically, avoid malicious software, respect digital rights and AI ethics
3	Confidence and privacy	Protect client, user and organisational data; prevent unauthorised access or disclosure
4	Competence	Maintain and update professional knowledge, ensure work is of high quality
5	Professional conduct	Treat colleagues, clients and users with respect and fairness; promote diversity and inclusion
6	Respect for intellectual property	Uphold copyrights, patents and licensing agreements; avoid unauthorised use

7	Public interest and social responsibility	Consider societal impact, contribute positively to the community
8	Continuing professional development	Keep up with technology and ethical practices, support lifelong learning in the computing community

Impacts of technology

- Social (lifestyle, communication, entertainment, health)
    - Positive
        - **Communication and connectivity:** Fosters collaboration and virtual communities, enables staying in touch across distances
        - **Entertainment and content access:** Digital platforms provide personalised, on-demand access to movies, music and television globally.
        - **Health and well-being:** Apps and wearable technology
        - **Convenience and safety:** Mobile apps can locate lost devices or help in emergency situations.
    - Negative
        - **Privacy concerns:** Tracking, personal data collection, targeted advertising without full consent
        - **Cyber risks:** Cyberbullying, harassment, hate speech, emotional harm via anonymous online communication
        - **Misinformation:** Rapid spread of false information on social media can lead to the erosion of trust and social division
        - **Addiction and mental health:** Excessive usage can cause social isolation, comparison stress, anxiety etc.

        - **Digital divide:** Socioeconomic and educational factors limit some people's access to technology.
            - To overcome this access inequality, we can promote digital inclusion through affordable access, training and support for marginalised communities.
        - To overcome **legal issues**:
            - Intellectual property — respecting copyrights, patents and digital content ownership
            - Cybersecurity and data privacy — implementing laws and regulations to protect information and digital assets
- Economic and workplace
    - Positive
        - **Efficiency and automation:** Streamlines processes and reduces manual tasks
        - **Collaboration and flexibility:** Tools like video conferencing, instant messaging and project management software enables remote teamwork and flexible work arrangements.
        - **Data-driven decisions:** Advanced analytics, AI and ML allow organisations to better analyse data and predict trends to make better decisions, as well as to optimise operations.
        - **New business models and jobs:** Technology enables the creation of new industries and roles.
            - e.g. Food delivery platforms create jobs for riders and drivers, while also changing consumer behaviour.
    - Negative
        - **Job displacement:** Automation, AI and robotics can replace traditional roles.

- **Skill shifts:** Workers need to adapt, upskill and embrace lifelong learning to remain relevant and employable.

@star.notes