[Unit 6] Seminar 3: Security Standards

A. The Importance of Security Standards

Regulations and standards applicable to organisations:

- International bank - PCI-DSS, GDPR (European-based)
- Large hospital - HIPAA, GDPR (European-based), PCI-DSS (website credit card payment)
- Large food manufacturing factory - HIPAA (food handling), GDPR, PCI-DSS

As a rule, refer to GDPR when a matter is EU-related, and as for PCI-DSS, it depends on payment method (i.e. credit cards).

B. Case Study 5: Disclosure of CCTV footage from a direct provision centre - RIA, Aramarkin

- Addresses *responsibilities of data processor* (company in charge of handling data).
- How was it resolved? The commissioner fined the company.
- Steps as an Infosec Manager to mitigate issue
    - Retraining staff
    - Implement [access] controls
    - Ensure job description includes data handling responsibly

Revelation: Since the company was registered as a data processor, it is the company responsible for GDPR (covers the company) and not the individual. However, if company staff has been trained yet did not follow regulations, it is

possible for the company to sue individual for the lack of judgement and non-compliance.

Aside: There was mention of a case of a person who escaped a fine for not cleaning up dog poo by arguing that CCTV cameras were not meant for that purpose as it intrudes privacy.

References

Data Protection Commission (2020) Case Studies: Data Protection Commission.

HIPAA (2020) HIPAA For Dummies – HIPAA Guide .

ICO (2020) Guide to the General Data Protection Regulation (GDPR).

PCI Security Standards.org (2020) Official PCI Security Standards Council Site - PCI Security Standards Overview.