Cybersecurity in industrial context

Lecture in IGBE01 – Production Management, part II

Samuel Wairimu, Karlstad University, Sweden

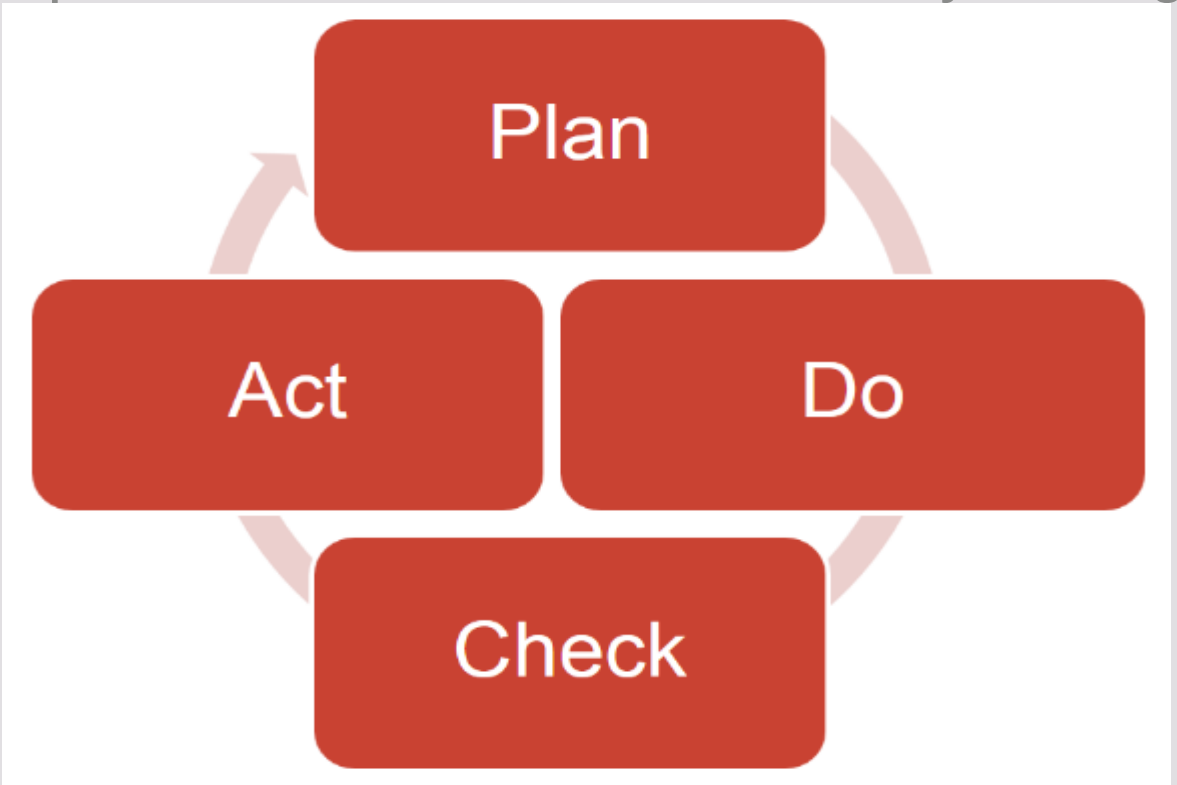
25th October 2021

Information Security Management System (ISMS) in ISO 27000

- ISO 27000 family of standards is usually relied upon by organizations when it comes to keeping information assets secure

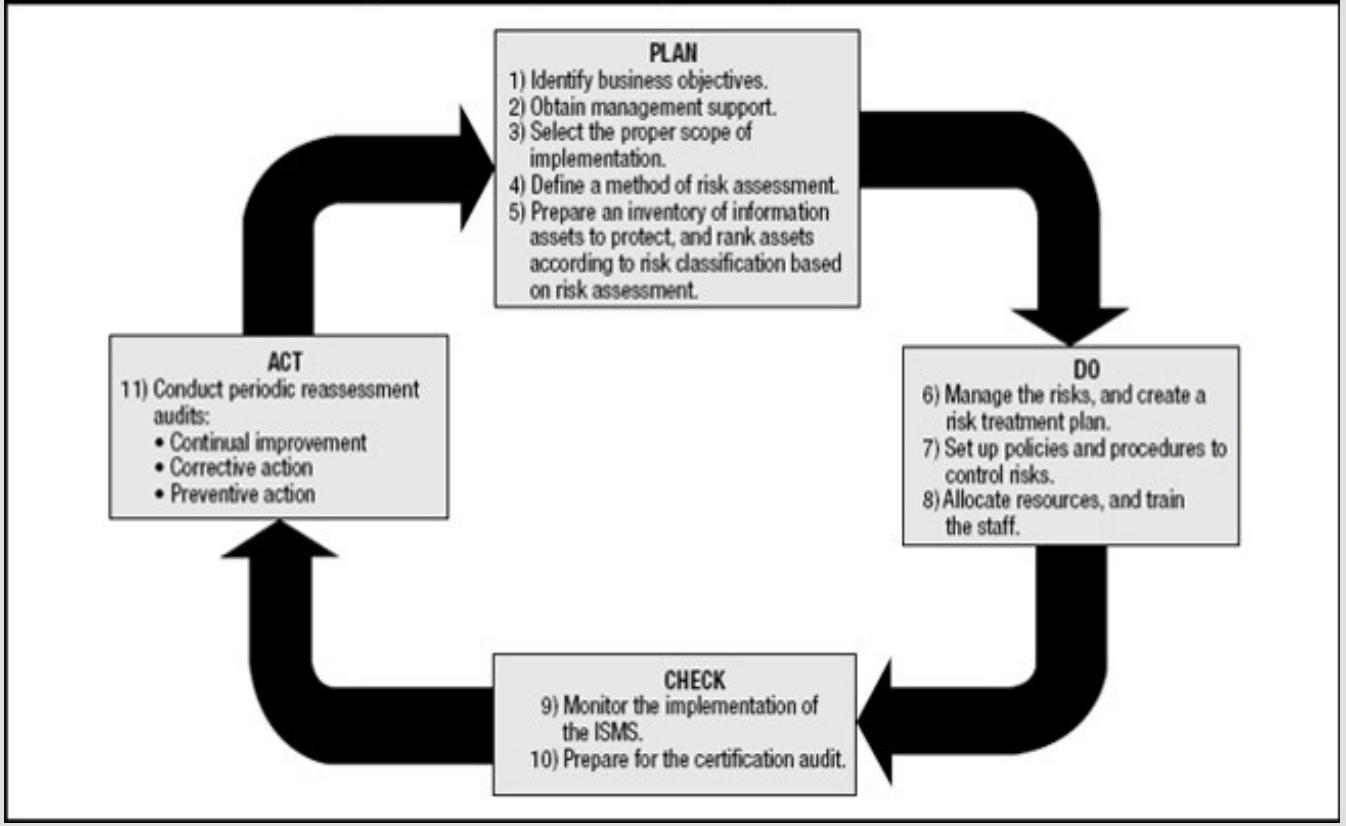
- ISO 27001:2013
    - Provides requirements for information management system (ISMS) and the assessment and treatment of information security risks tailored to the needs of the organization.
    - The requirements set out in ISO 27001 are generic and are intended to be applicable to all organizations, regardless of type, size or nature.
    - It incorporates the PDCA cycle

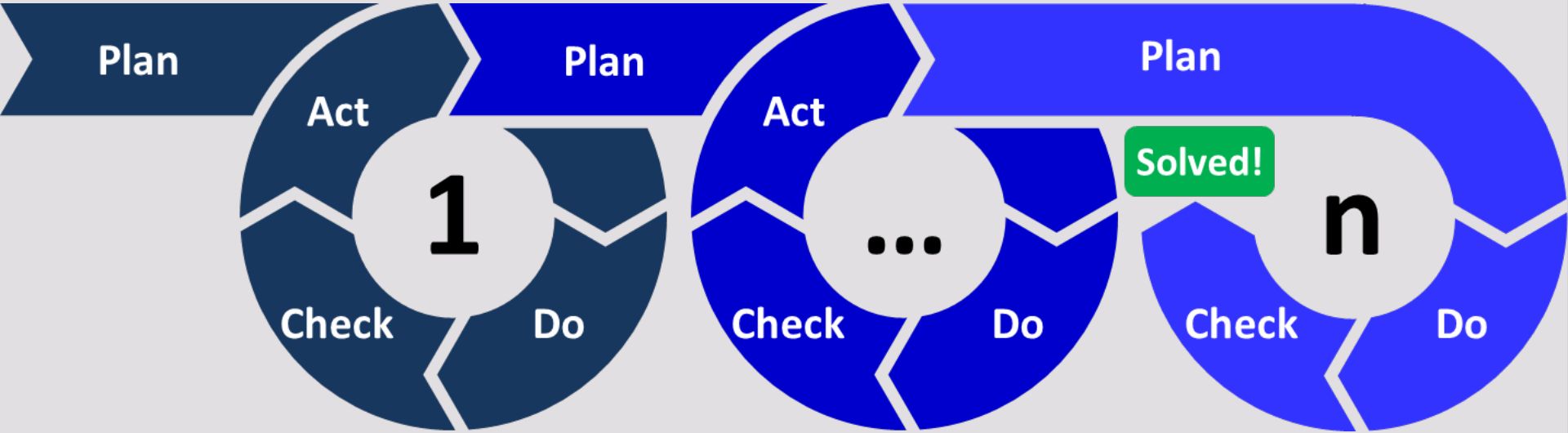
Privacy Impact Assessment in Info Security Management



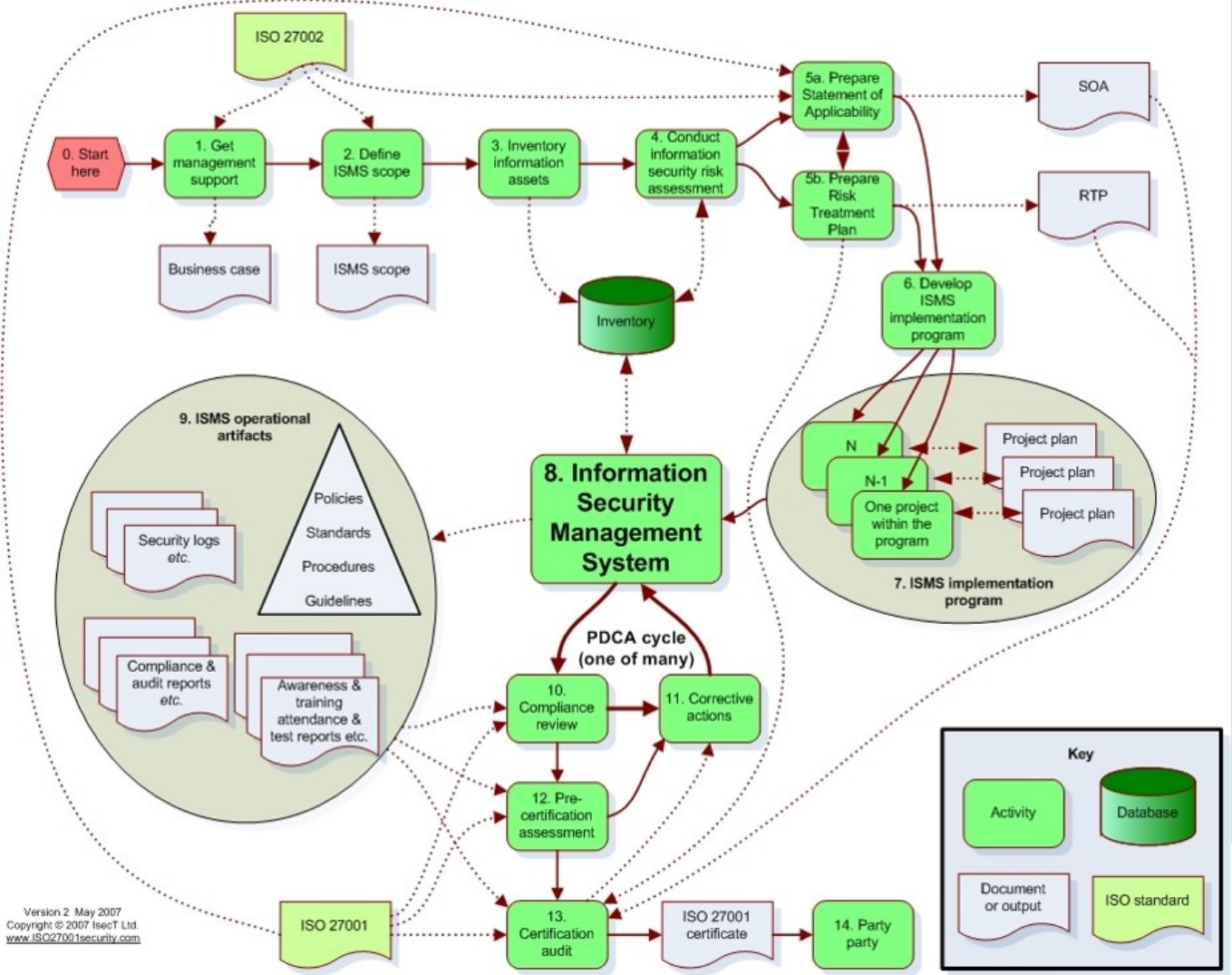
Samuel Wairimu
Department of Mathematics and Computer Science

Figure 1—PDCA Cycle and Respective Implementation Phases





Samuel Wairimu
Department of Mathematics and Computer Science



References

- http://www.iso27001security.com/
- "Planning for and Implementing ISO 27001" by Charu Pelnakar, ISACA Journal, Vol. 4, 2011
- Mapping between GDPR (the EU General Data Protection Regulation) and ISO27k, Iso27k forum, November 2016

Organizing the ISMS

- Get management support & budget!
- Set up ISMS panel with participation of relevant roles:
  - Head of IT
  - Management
  - Head of Production
  - IT security managers
- Regular meetings (e.g., monthly) where incidents are analyzed and priorities get defined.
- Define triggers that cause re-assessment!

Stakeholders

The Players

- The Board
- The CEO
- The Forum

The Subjects

- Humans
- Assets
  - Equipment
  - Networks
  - Applications
  - Information Stores

The Process

- Establish/Upgrade controls
- Reporting and Monitoring
- Continued evaluation
- Corrective actions

The Documents

- Policy
- Procedures for handling
  - Assets
  - Incidents
  - People
- Detailed routines as appropriate

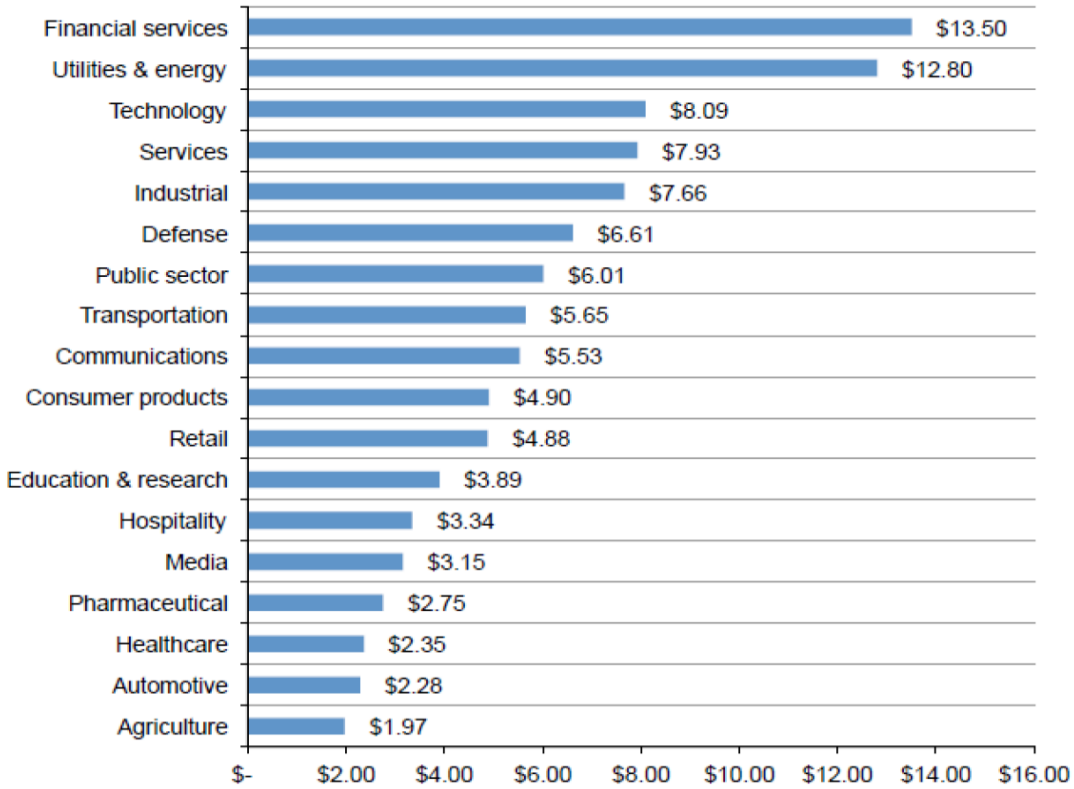
Triggers for re-assessment

- Internal changes in infrastructure
- New software installed
- New suppliers
- Outsourcing to subcontractors
- Major software updates
- Major staff changes or other corporate events (lay-offs, competence loss)
- Changes in physical location
- Product updates or new products
- ”World change”: Newly discovered risks, hacking tools, attacks, crypto analysis

Cost of information security incidents

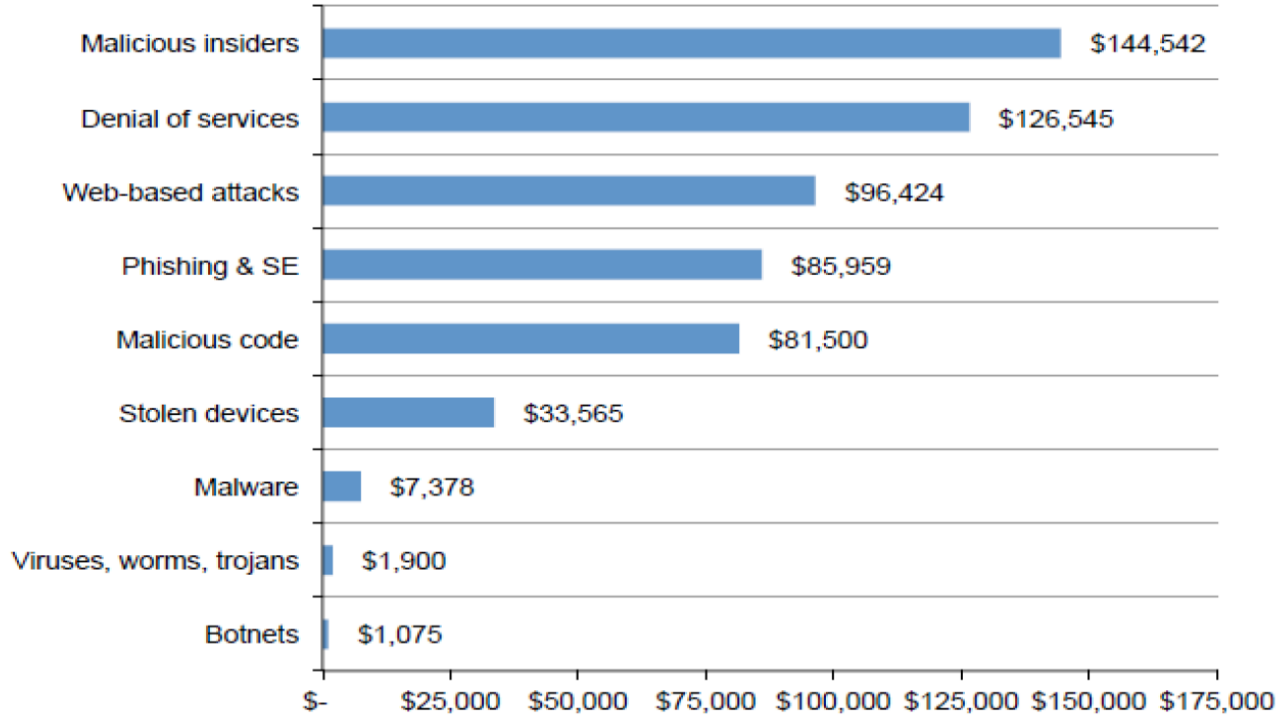
- Examples from ENISA report on cost of incidents
- Privacy breaches and their cost

Figure 6: Average annualized cost by industry sector (millions) [16]



ENISA: The cost of incidents affecting CIIs, 2016

Figure 9: Percentage annualized cybercrime cost, by attack type [16]



ENISA: The cost of incidents affecting CIIs, 2016

Figure 8: Attack/Threat types per CII sector (graphical view of Table 2)

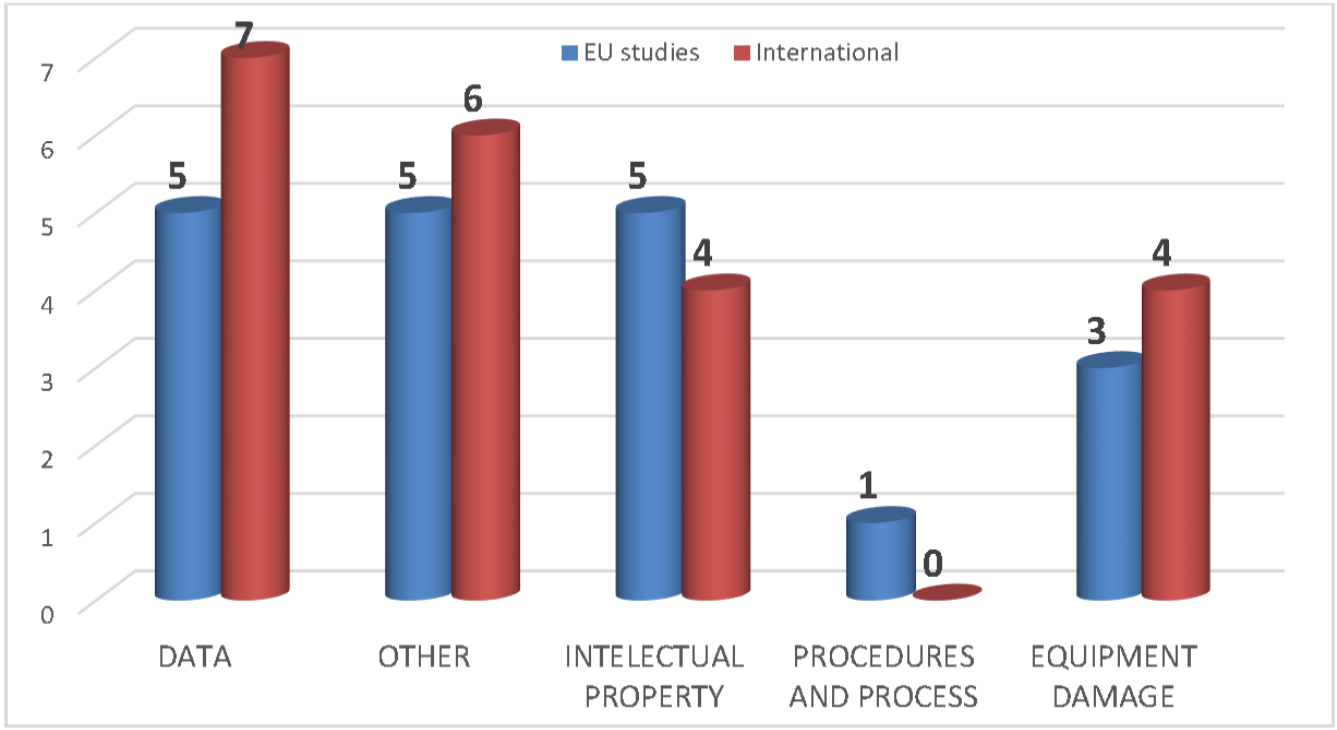
Table 2: Attack/Threat types per CII sector

Nr.	Attack / Threat	Number of studies per sector									
		Public Administration	Energy	Health	Financial	ICTs	Transport	Water	Aerospace	Food	Chemistry
1	Malware	7	10	7	9	9	7	1	1	1	1
2	DoS/DDoS	10	8	8	11	11	8	1	1	1	–
3	Cyber Espionage	2	3	3	3	2	1	1	1	–	1
4	Web-Based Attacks	5	7	4	7	7	6	–	1	1	–
5	Insider Threat	7	4	6	8	7	3	–	1	1	–
6	Hacktivism	3	3	3	5	4	–	–	1	1	1
7	Malicious Code	5	6	5	7	7	6	–	–	–	–
8	Phishing	6	4	4	6	6	4	1	–	–	–
9	Web Application Attacks	5	2	4	4	4	2	1	–	–	–
10	Ransomware	3	1	3	2	2	1	1	–	–	–
11	Botnets	1	2	2	2	2	2	–	–	–	–
12	Critical Vulnerabilities	1	1	1	–	–	1	1	–	–	–

ENISA: The cost of incidents affecting CIIs, 2016

Samuel Wairimu
Department of Mathematics and Computer Science

Figure 10: Assets affected



ENISA: The cost of incidents affecting CIIs, 2016

The World’s Biggest Data Breaches

Collection of large known personal data losses:

http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

Business side cost factors of privacy management

***Privacy Office*:** Costs associated with dedicated staff, office overhead, travel and business equipment.

Policy & Procedures: Costs associated with the creation, review, publication and dissemination of the privacy policy (and privacy notice when applicable).

***Downstream Communications*:** Costs associated with the communication and outreach activities for the privacy program both within the company and to outside stakeholders.

***Training & Awareness*:** Costs associated with the education of employees and other key company stakeholders about the privacy policy, program and related concepts.

***Enabling Technologies*:** Costs associated with technologies that help mitigate privacy risk, enhance responsible information management, or protect the critical data infrastructure.

Employee Privacy: Costs associated with the protection of sensitive employee records, including heath care and OSHA claims.

***Legal Activities*:** Costs associated with legal review and counsel concerning the privacy program as well as legal defence costs in the event of a privacy violation.

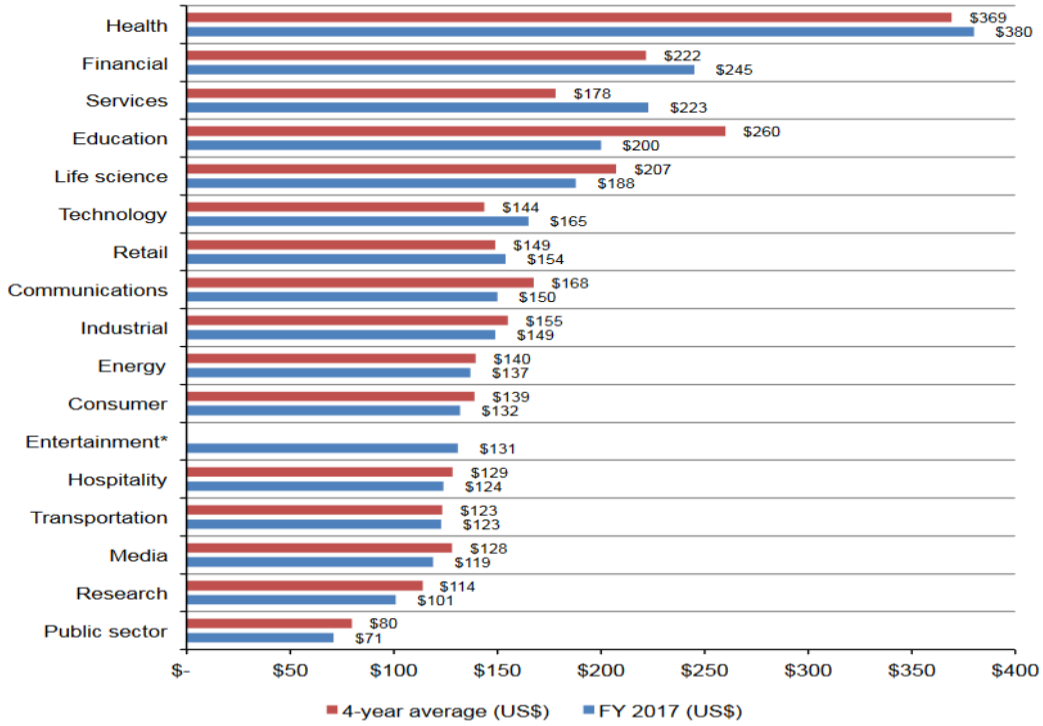
***Audit & Control*:** Costs associated with the monitoring, verification and independent audit of the privacy program, including use of controlled self-assessment tools.

***Redress & Enforcement*:** Costs incurred to provide upstream communication of a privacy or data protection breach to appropriate parties within the organization, including the cost of investigation and collaboration with law enforcement. In addition to the above cost center activities, the current research captured additional information

Ponemon Institute, "2017 Cost of Breach Study" - Global Overview", 2017

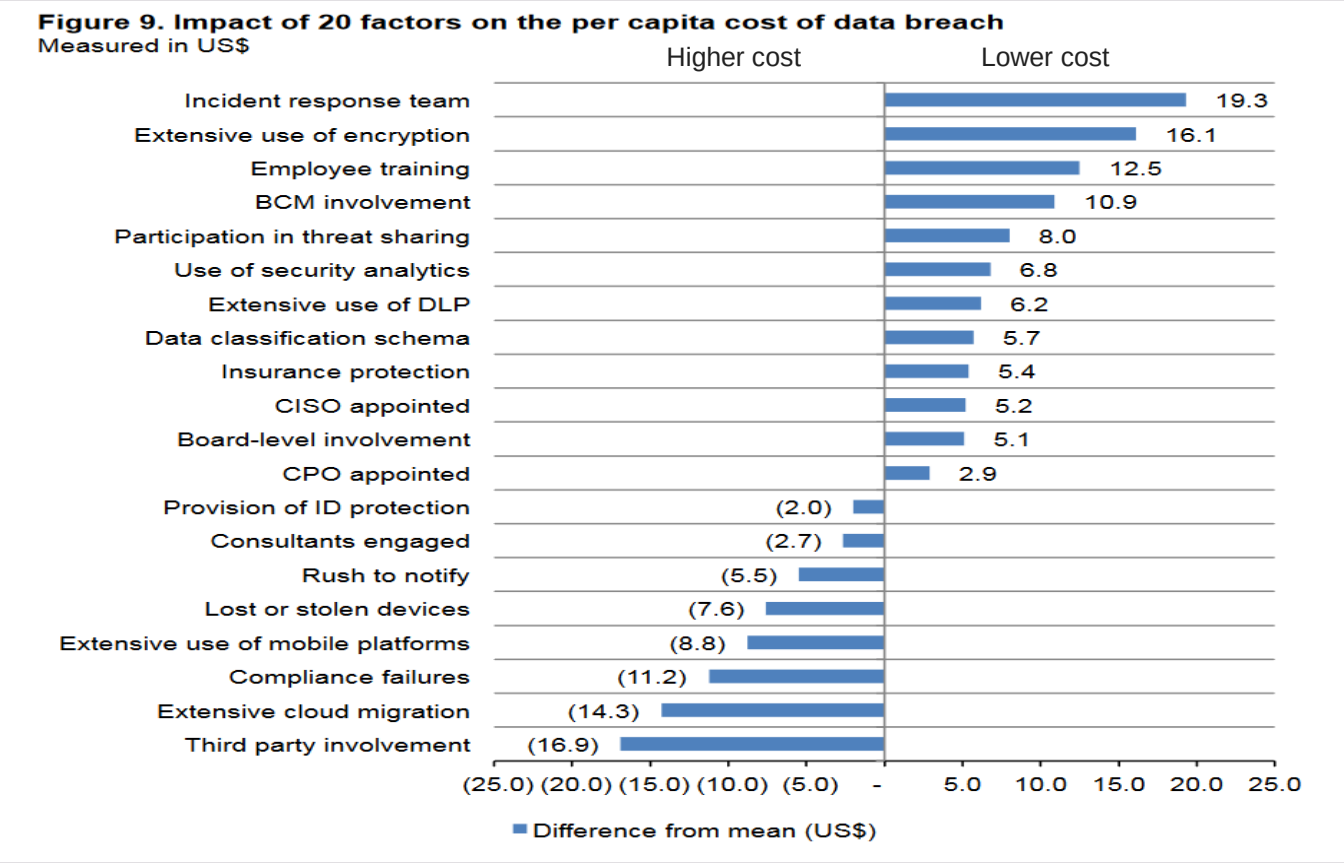
"Cost of privacy" from (Ponemon, 2004).

Figure 5. Per capita cost by industry classification
*Historical data are not available for all years
Measured in US$



Samuel Wairimu
Department of Mathematics and Computer Science

Ponemon Institute, "2017 Cost of Breach Study" - Global Overview", 2017



Ponemon Institute, "2017 Cost of Breach Study" - Global Overview", 2017

Summary

- IT security management manages risks related to data and systems.
- Risks cause disruption, direct cost and risk handling cost.
- IT security management is a complex process that involves many parts of an organization, their suppliers and the basic communication and IT infrastructures they use.
- Personal data is a special class of information assets.
- Production or delivery of services is critically dependent on IT.
- IT security investments are investments that pay off by preventing and reducing incident cost.