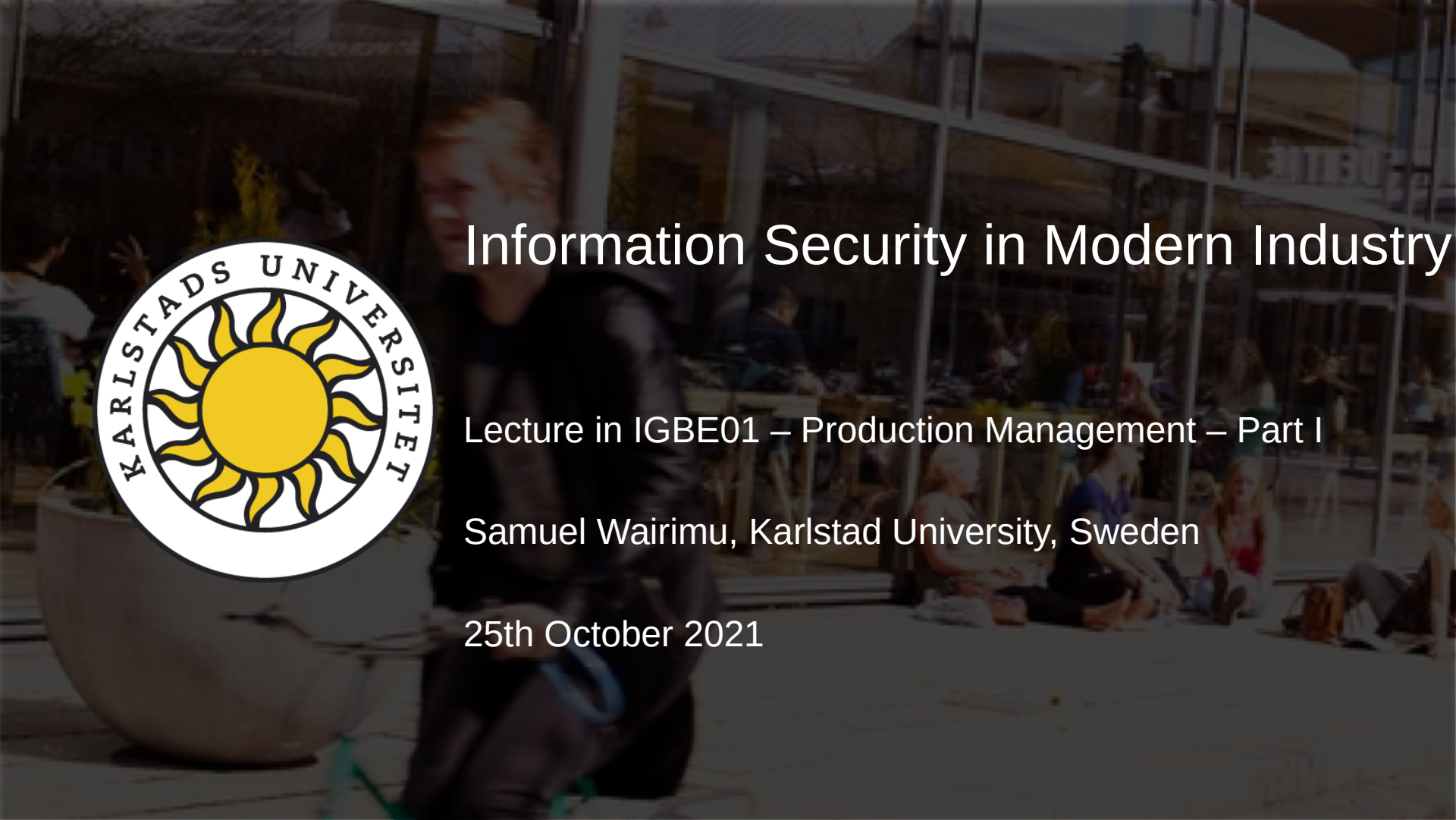


Information Security in Modern Industry

Lecture in IGBE01 – Production Management – Part I

Samuel Wairimu, Karlstad University, Sweden

25th October 2021

About me

- PhD Student in the Computer Science – Department of Mathematics and Computer Science.
- Graduated with a Master’s Degree in Cyber security from the University of Chester (Chester, England).
- Focus:
    - Privacy and Security of IT-based Systems in Healthcare
- Research Interests: Information security and privacy, cyberwarfare, cyber security, Digital Health

Contents

- Information security as part of the management process
  - IT going down: Maersk's cyber crisis
  - How is information security related to industrial production?
  - Product, data and critical infrastructures
  - Security risk analysis and privacy impact analysis
- Case study: connected car production security risk
  - Introduction of a production scenario
  - Identification of information assets and risks
  - Selection of controls
- Information Security Management System (ISMS) in ISO 27000
  - A standard for corporate information security management as part of IT management

Lecture Goals

- The lecture will be a high-level introduction to information security and risk assessment. Focus will be put on information security in relation to industrial production.
- Learning goals:
    - Participants shall develop a general understanding of risk analysis which is based on likelihood and impact of realized threats.
    - Participants shall understand the basic ideas of threats, threat actors, attacks and their consequences.
    - Participants shall gain insight into subjectivity of decision-making in such assessments – through a case study: connected car production security risk
- Introduction to the ISO 27000 family of standards with a focus on ISO 27001

What is information security?

Samuel Wairimu
Department of Mathematics and Computer Science

Information security is…

- … is expressed through three properties of systems and data:

C-I-A

Data or systems are only readable or accessible to those who are authorized to do so.

Data or systems remain in original state – they do not become changed in ways not authorized.

Data or systems are available as needed.

Information security cont...

- But what if the security goals are undermined by threat actors?

	AGENT LABEL	DEFINING MOTIVATION	PERSONAL MOTIVATION
EXTERNAL	Hacktivist	✓ Ideology	✓ Ideology
	Competitor	✓ Organizational Gain	✓ Personal Financial Gain
	Cyber Vandal	✓ Dominance	✓ Dominance
	Data Miner	✓ Organizational Gain	✓ Personal Financial Gain
	Online Social Hacker	✓ Personal Financial Gain	✓ Personal Financial Gain
	Script Kiddies	✓ Personal Satisfaction	✓ Personal Financial Gain ✓ Personal Satisfaction
	Government Cyber-warrior	✓ Dominance	✓ Ideology ✓ Personal Financial Gain ✓ Personal Satisfaction
	Organized Crime	✓ Organizational Gain	✓ Personal Financial Gain ✓ Coercion
	Radical Activist	✓ Ideology	✓ Ideology
	Sensationalist	✓ Notoriety	✓ Personal Satisfaction
	Cyber Terrorist	✓ Ideology	✓ Ideology
	Car Thief	✓ Personal Financial Gain	✓ Personal Financial Gain ✓ Personal Satisfaction
	Information Partner	✓ Organizational Gain	✓ Personal Financial Gain
INSIDER	Government Spy	✓ Ideology	✓ Ideology ✓ Personal Financial Gain ✓ Personal Satisfaction
	Internal Spy	✓ Personal Financial Gain	✓ Ideology ✓ Personal Financial Gain ✓ Coercion
	Disgruntled Employee	✓ Disgruntlement	✓ Disgruntlement
	Reckless Employee	✓ Accidental	✓ Accidental
	Untrained Employee	✓ Accidental	✓ Accidental
	Outward Sympathizer	✓ Personal Satisfaction	✓ Personal Satisfaction

Maersk crisis

- What had happened?
- What were the consequences for Maersk’s production of transport?
- What were the reasons for the stop in production?

Samuel Wairimu
Department of Mathematics and Computer Science

Information security is a part of production

- Most processes controlled by IT today.
  - Physical production, digital services, supply on demand, power networks, transport.
  - Control systems, production robots, telemetry and remote control, dynamic configurations, data-dependent production, data products.
- Real-time connection.
- Global exposure, global value chains.

IT security management is a horizontal activity

- Part of quality management (product and service quality depend on IT quality)
- Part of operations management (IT runs production)
- Part of procurement (security requirements when sourcing cloud services)
- Part of HR management (planning, recruiting, training, dispatching of staff)
- Part of facility management (physical security of IT components)
- Part of logistics (both on way in and on way out)
- Part of sales (web shops, digital procurement)
- Part of finances (payment, billing, taxation, customs)

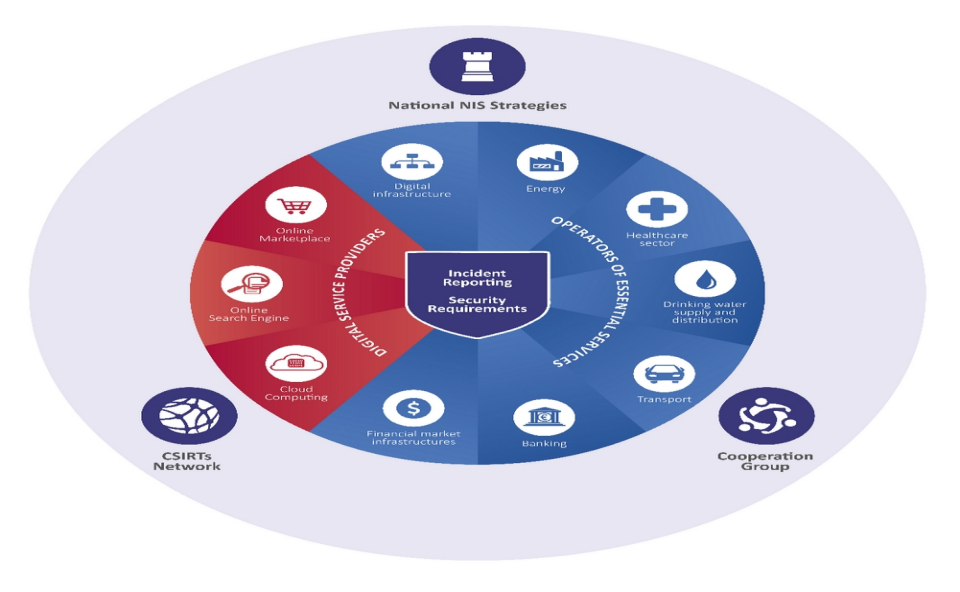
Most departments and functions will have contact with IT security management.

Critical infrastructures

- Information and communication infrastructures and depending physical infrastructures considered essential for society's normal function.
  - Communications infrastructure
  - Energy production & distribution
  - Healthcare services
  - Water supply
  - Transport infrastructure
  - Banking, Payment and financial market infrastructure
- Originally inspired by cyberwar threat, term came to life after Russian cyber attack on Estonia in 2007.
- Interestingly, digital media distribution not explicitly mentioned – think of fake news, election influence campaigns, troll armies with political goals.

EU’s NIS directive to protect critical infrastructure

- ”Network and information security directive”, Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union
  https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive



Core elements:

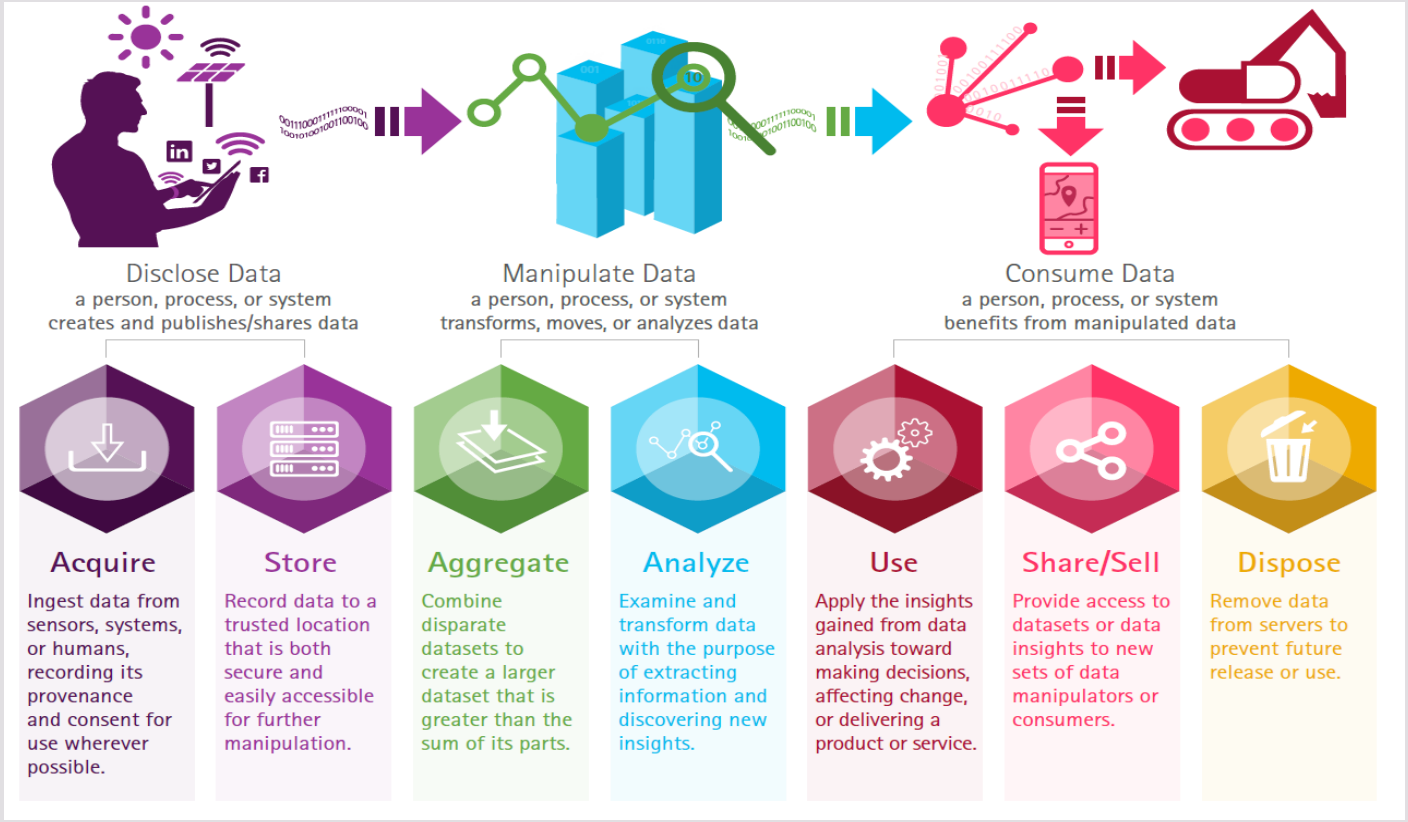
- Mandatory incident reporting
- IT Security requirements
- Regulatory requirements
- Incident response teams
- Collaboration between governments and private actors

Samuel Wairimu
Department of Mathematics and Computer Science

Image: Enisa,

Data is the new oil … what about the oil spills?

- Massive data collection, analysis and distribution capacity
- ”Big Data” promises near-magic self learning, knowledge-discovering and artificially intelligent computers – if they just get fed enough information.
- Data leakage, data sabotage, espionage and poor data quality are serious threats
- Hard to revert a ”data spill” once data has leaked, been stolen or published.
  Think about the 1177.se phone calls leak!
  What customer risks may happen?
- Data protection regulation defines rules about how personal data must be processed
- IT risk management should deal with privacy risk, too!



Accenture report: Building digital trust: The role of data ethics in the digital age, https://apo.org.au/node/71946 , accessed October 2021

IT security risk assessment

- A process that identifies assets at risk, threats, and potential for risks occurring.

Risk Assessment is a systematic study of
- assets
- threats
- vulnerabilities
- and impacts (consequences)

to assess the probability and consequences of risk

- Risk Management is a formalized process;
  - planned
  - input data recorded
  - analysis and results should be recorded

Qualitative risk assessment

- Uses likelihood and impact of events on assets
- Based on historic data for both likelihood and impact
- In new settings often guesswork

Loss(A) = impact(T(A))*likelihood(T(A)) where T(A) is threat T effective on asset A.

Risk assessment form

Likel / Imp	Negli	V low	Low	Med	High	V High	Extr
None							
Minor							
Med							
High							
V High							
Extr							

Three levels of risk are normally adequate: low, moderate, high

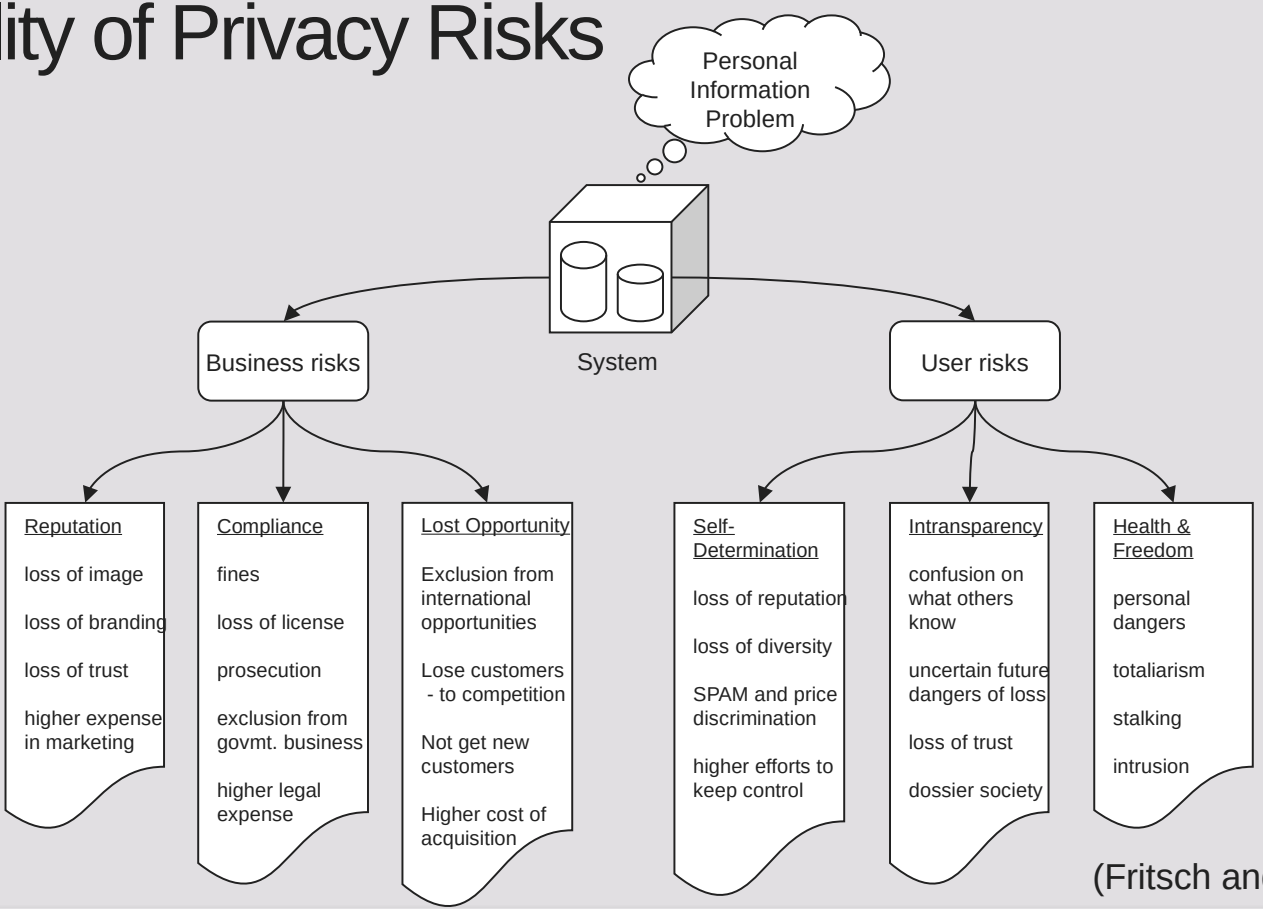
Assessment of privacy risk and impact

- **Risk**:
  What might happen – and how often. How many will be affected?
  Classic security risk analysis: How hard will it hit us (low, medium high)?

- **Impact**:
  Impact on the data subject, its environment and surrounding society.

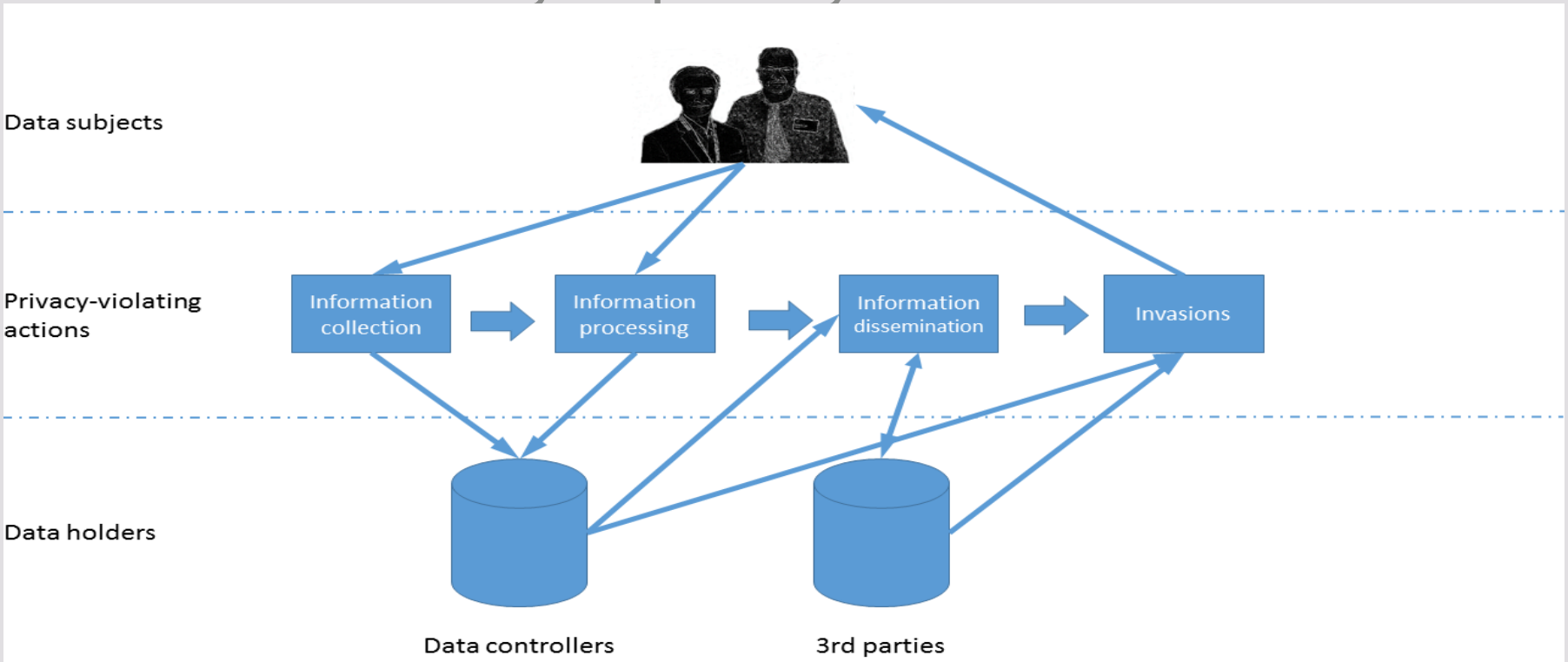
- Privacy Impact Analysis / Data protection impact analysis is required by data protection regulation for all systems that collect, process or store sensitive personal data or large amounts of data about many persons.

Duality of Privacy Risks



(Fritsch and Abie 2008)

Solove's taxonomy of privacy violations



D. Solove, "A taxonomy of privacy," *University of Pennsylvania Law Review,* vol. 154, pp. 477-564, January 2006

ENISA PIA Impact Levels

The European Union Agency For Network and Information Security (ENISA) has published guidelines for privacy risk assessment for Small and Medium Enterprises that contain guidance on privacy impact assessment focused on individual data subjects in chapter 3 on page 19. There, four levels of privacy impact are defined:

LEVEL OF IMPACT	DESCRIPTION
Low	Individuals may encounter a few minor inconveniences, which they will overcome without any problem (time spent re-entering information, annoyances, irritations, etc.).
Medium	Individuals may encounter significant inconveniences, which they will be able to overcome despite a few difficulties (extra costs, denial of access to business services, fear, lack of understanding, stress, minor physical ailments, etc.).
High	Individuals may encounter significant consequences, which they should be able to overcome albeit with serious difficulties (misappropriation of funds, blacklisting by financial institutions, property damage, loss of employment, subpoena, worsening of health, etc.).
Very high	Individuals which may encounter significant, or even irreversible consequences, which they may not overcome (inability to work, long-term psychological or physical ailments, death, etc.).

ENISA: Guidelines for SMEs on the security of personal data processing, December 2016, ISBN 978-92-9204-209-7, DOI 10.2824/867415, European Union Agency For Network and Information Security.

ENISA x SOLOVE

	Collect	Process	Disseminate	Invade
Publication of personal annual tax lists to the public	[LOW]	[MEDIUM]	[HIGH]	[VERY HIGH]
	Individuals may encounter a few minor inconveniences, which they will overcome without any problem (time spent re-entering information, annoyances, irritations, etc.).	Individuals may encounter significant inconveniences, which they will be able to overcome despite a few difficulties (extra costs, denial of access to business services, fear, lack of understanding, stress, minor physical ailments, etc.).	Individuals may encounter significant consequences, which they should be able to overcome albeit with serious difficulties (misappropriation of funds, blacklisting by financial institutions, property damage, loss of employment, subpoena, worsening of health, etc.).	Individuals which may encounter significant, or even irreversible consequences, which they may not overcome (inability to work, long-term psychological or physical ailments, death, etc.).

Evaluation of Risk: ENISA Guidelines for SMEs

Figure 4: Final risk evaluation

The population of the risk matrix below with risk levels was performed on the assumption of the worst-case scenario (highest possible impact on the individual). Consequently, the impact level was weighted more than the threat occurrence probability and only two low risk and three medium risk levels have been identified. High and Very High Impact levels have all been assigned to high risk levels and have been merged.

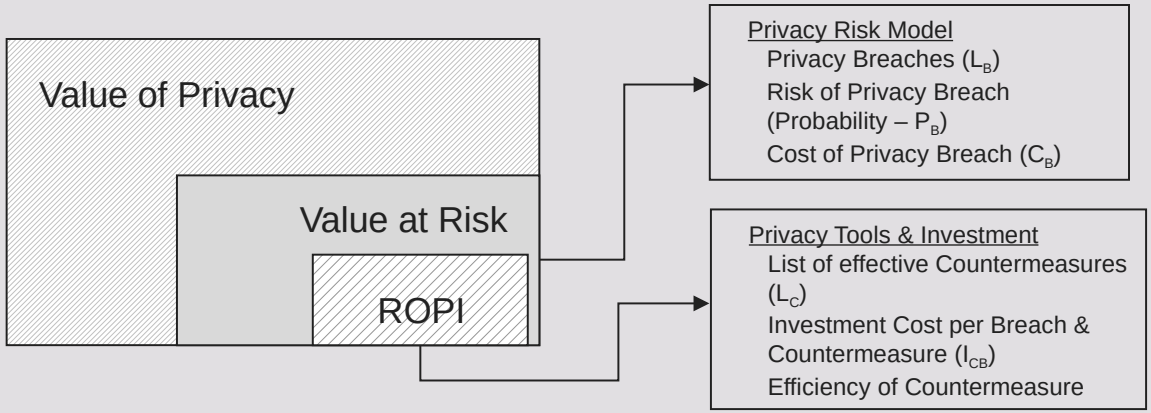
		IMPACT LEVEL		
		Low	Medium	High / Very High
Threat Occurrence Probability	Low			
	Medium			
	High			

Legend

Low Risk *Medium Risk* *High Risk*

ENISA: Guidelines for SMEs on the security of personal data processing, December 2016,
ISBN 978-92-9204-209-7, DOI 10.2824/867415,
European Union Agency For Network and Information Security.

Business view: Return On Privacy Investment ROPI



Value_after_investment = Value_of_Privacy – (Value_at_Risk – ROPI) where for any privacy breach L_B : $ROPI = P_B * C_B - I_{CB}$

(Fritsch and Abie, 2008)

Problem with ”cost per privacy breach”

- What is the specific cost? Who pays the cost?
- Risk management usually is used by service providers, system owners, or in general businesses to minimize their own losses.
- Customers’ losses, or data subject’s losses are not necessarily losses for the system owner.
- Regulation (laws and fines) are often used to align data subject losses with corporate losses in case of corporate misbehavior

Drawbacks

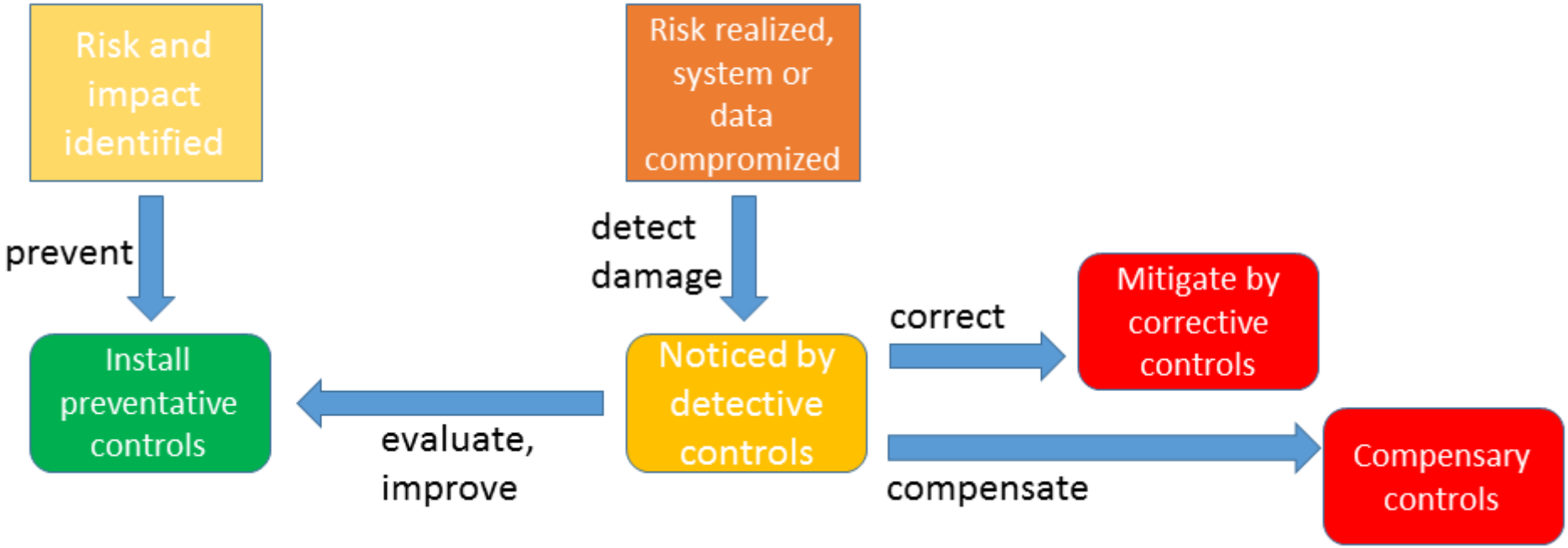
- Lack of quantified data (cost & occurrence of incidents, effective & cost of PET)
  - Legislation on mandatory reporting of data breaches
- Lack of long-term privacy risk model (duality!)
- Much ”expert guessing” necessary
  - Good for expert’s hourly rates
  - Bad for scientific accuracy

Security and privacy controls

- To reduce or remove a risk we chose appropriate controls that treat risks.
- Choose e.g. privacy controls. Example: NIST 800-53 and Privacy Overlay.

- CNSSI 1253F, Attachment 6: Privacy Overlay, 04/23/2015
- NIST SP 800-53 Rev.5: Security and Privacy controls for information systems and organisations
- M. Colesky, J. H. Hoepman, and C. Hillen, "A Critical Analysis of Privacy Design Strategies," presented at the Workshop on Privacy Engineering IWPE'16, San Jose, USA, 2016

Types of security and privacy controls



NIST privacy controls

- NIST Special Publication 800-53 on Security and Privacy Controls for Information Systems and Organizations is the specification of privacy and security controls for public offices in the United States.

- It contains an extensive collection of specified controls including appendices that show how to select controls that respond to various risk and impact levels.

- These controls can be found in chapter 3 under The Controls (NIST Special Publication 800-53 Rev 5)

NIST Privacy Controls

TABLE 1: SECURITY AND PRIVACY CONTROL FAMILIES

ID	FAMILY	ID	FAMILY
AC	Access Control	PE	Physical and Environmental Protection
AT	Awareness and Training	PL	Planning
AU	Audit and Accountability	PM	Program Management
CA	Assessment, Authorization, and Monitoring	PS	Personnel Security
CM	Configuration Management	PT	PII Processing and Transparency
CP	Contingency Planning	RA	Risk Assessment
IA	Identification and Authentication	SA	System and Services Acquisition
IR	Incident Response	SC	System and Communications Protection
MA	Maintenance	SI	System and Information Integrity
MP	Media Protection	SR	Supply Chain Risk Management

Summary on privacy risk

- PIA is focused on the worst-case impact on the individual.
- PIA is ”foreseeing the possible bad future”
- PIA needs good insight into threats, mistakes, side effects and the resulting personal consequences in various ”life contexts”

- Treatment of privacy risks and impact is an extensive process changing infrastructure and processes with privacy controls that demands resources, knowledge and priority in corporate information security management.

Resource problem for smaller companies. Recommendation:

- Minimize personal data collection to the bare necessities.
- Stick to a particular purpose – more flexibility creates more complexity in PIA .