Classification: Public

Risk Management for Cloud, Computing, and Data Services

GÉANT SIG-ISMS Workshop
Copenhagen Feb 22-23, 2016

Urpo Kaila, <kaila@csc.fi>
EUDAT Security Officer,
SIG-ISMS WG chair,
Head of Security@CSC)

EUDAT receives funding from the European Union's Horizon 2020 programme - DG CONNECT e-Infrastructures. Contract No. 654065

Overview

- What is risk management - for real?
- Mitigation, ownership and learning from incidents
- Business Impact Analysis (BIA)
- How to make risk management operational?
- Risk Management in specific areas
  - Computing
  - Cloud
  - Data Services
- Suggestions for practical improvements at your site
- Could we do something together?

What is risk management?

- By addressing risks, uncertainties and opportunities through an Enterprise Risk Management (ERM) framework organisations can protect shareholder and stakeholder value
- Risk management is one of the most important tasks for management - but often widely neglected or misunderstood
- Typical areas for ERM are strategic risks, financial risks, operational risks, and damage risks (terms my vary depending of framework)
- TyA risk register can be a good tool to share information about risks
  - EUDAT Risk Register

ERM phases

- Typical phases in ERM are:
  - Defining risk context and defining ERM framework
  - Identifying risks
  - Risk assessment by defining ownership, mitigation, transference, and retention/ acceptance
  - Monitoring and reviewing risks

ERM and Information Security Risks

- Information Security Risks Management is a subset of ERM
- For NRENs, Data Centres, and Computing Centres Information Security Risks are of a high importance – but do not forget other ERM related risks
- Many public and not-public standards and best practices available:
  - NIST 800-37, 800-39
  - $(ISC)^2$ CBK
  - ISACA COBIT and IT Risk related Guidelines
  - ISO 31000 series

BIA

- Business Impact Analysis is the most critical factor in Risk Management
  - How to 'translate" operational and damage risks to strategic risks?
  - BIA is the method to make communication between senior management and operation work
  - BIA should be based on facts and metrics, but typically it also requires tacit knowledge, experience and good communication skills

Risk Management and Compliance/Governance

- Organisations do risk management out of self interest to protect shareholders (or equivalent) and stakeholder value
- Risk Management is also explicitly required by most Information Security Management Frameworks and best practices
  - If you do not efficiently deploy risk management you do not comply. Period.
- In ISO/IEC 27001 the requirements for Risk Management are very specific – and a common source for non-compliance

Requirement for Risk Management in ISO/IEC 27001 (simplified version)

The organization shall define and apply an information security risk assessment process that:

a) establishes and maintains information security risk criteria

b) ensure that risk assessments produce consistent result

c) identify the information security risks and risk owners

d) analyze consequences and likelihoods of the risks

e) evaluates and prioritize the risks for treatment

The organization must retain documented information about the information security risk assessment process.

Terms for Quantitative Risk Analysis

SLE, Single Loss Expectancy = Asset Value (€)* Exposure Factor (EF)

EF, Exposure Factor is the effect of of loss would have on a asset

ARO, Annualized Rate of Occurrence is the estimated frequency of risks occurrence

ALE, Annualized Loss Expectancy = ARO X SLE

Example: Stolen laptops, replacement cost

Asset Value = € 1000

EF= 120 %

SLE = € 1200

ARO = 4

ALE = 4 x €1200 = € 5000

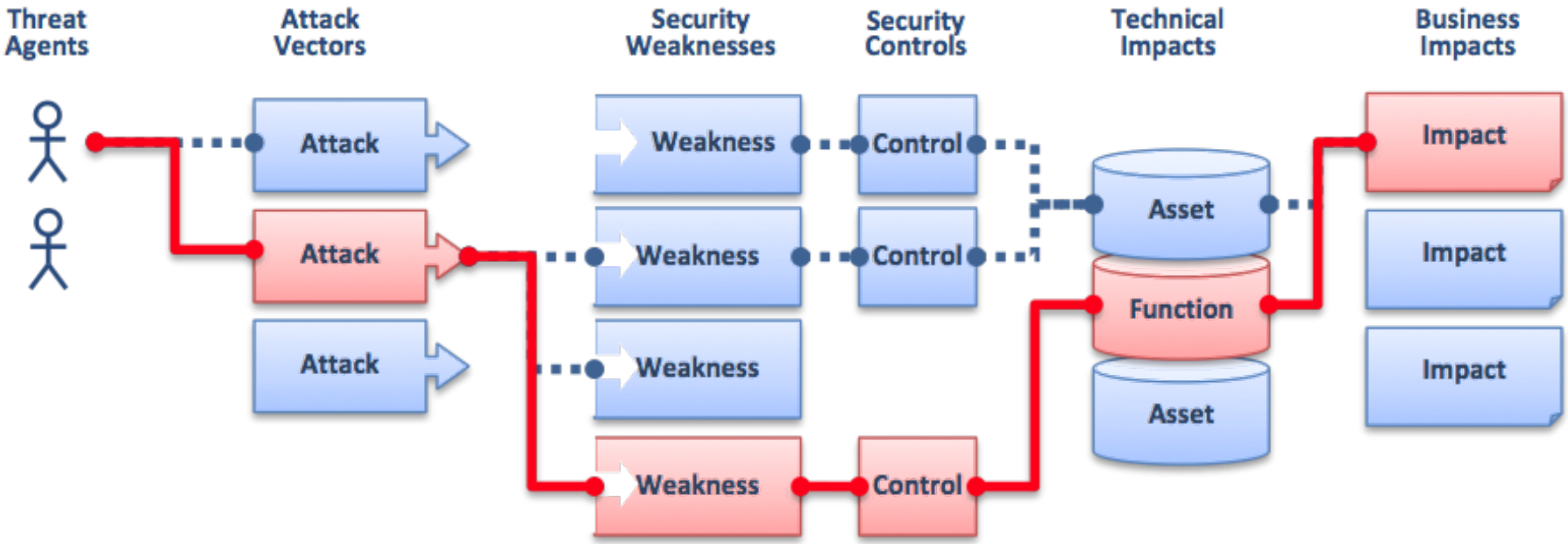
Would it make sense to insure the 100 company laptops against theft (risk transference) for a total of € 15 000 per year? Perhaps not.

* Or DKK here in Denmark ;)

Qualitative risk management

- Interviews
- Brainstorming
- SWOT
- Historical analysis
- Understanding
- Literary reviews
- Scientific articles

OWASP Risk Framework



OWASP CISO AppSec Guide: Criteria for Managing Application Security Risks

Common failures in Risk Management

- Risk management does not exists
- Risk management is not operational
- Risk ownerships are not implemented
- Management is not committed to risk management
- Risk management procedures are undocumented
- Risk are not reviewed or approved by management
- Unable to implement advance Risk management framework to smaller organisations
- Unable to connect costs and benefits
- No interconnection between ERM and IT Rsks/Operational and Damage risks
- Missing communications with comptroller
- Missing executive sponsor
- Missing a skilled, motivated and authorised risk manager/ chief risk officer

How to make risk management operational?

- Fix the issues mentioned on previous slide!

Common Basic Failures in Risk Management

- Misunderstanding of risk appetite/ risk aversion of the business

Common Very Basic Failures in Risk Management

- Aiming for perfection at once

Risk Management in specific areas

Risk context in research/computing/NREN oriented sites

- Often publicly funded (in Europe at least)
- Good and solid historical reputation, plenty of implicit trust - "A gentlemen's club"
- Often managed as academia, the "professors"/teams have strong autonomy
- Some employees are very skilled
- Mostly non-documented processes
- Non-profit and cost-efficient
- A good culture, mostly high morale
- Customer service can sometimes be edgy
- IT services are very open
- Open source software is widely used
- Now turmoil in funding, competition, technology and big cloud players seen as alternatives

IT Risk management for computing services (a very simple example)

Start with documenting and communicating the very basic risks (skip PR risks for now)

Event	SLE ("1-5")	ARO ("1-3")	ALE
A stolen account	n	m	n x m
Remote root exploit			
Staff abuse			
Data leakage			
Downtime due infrastructure/ HW/ SW issues			
System compromise			
Legal issues			
Funding issues			

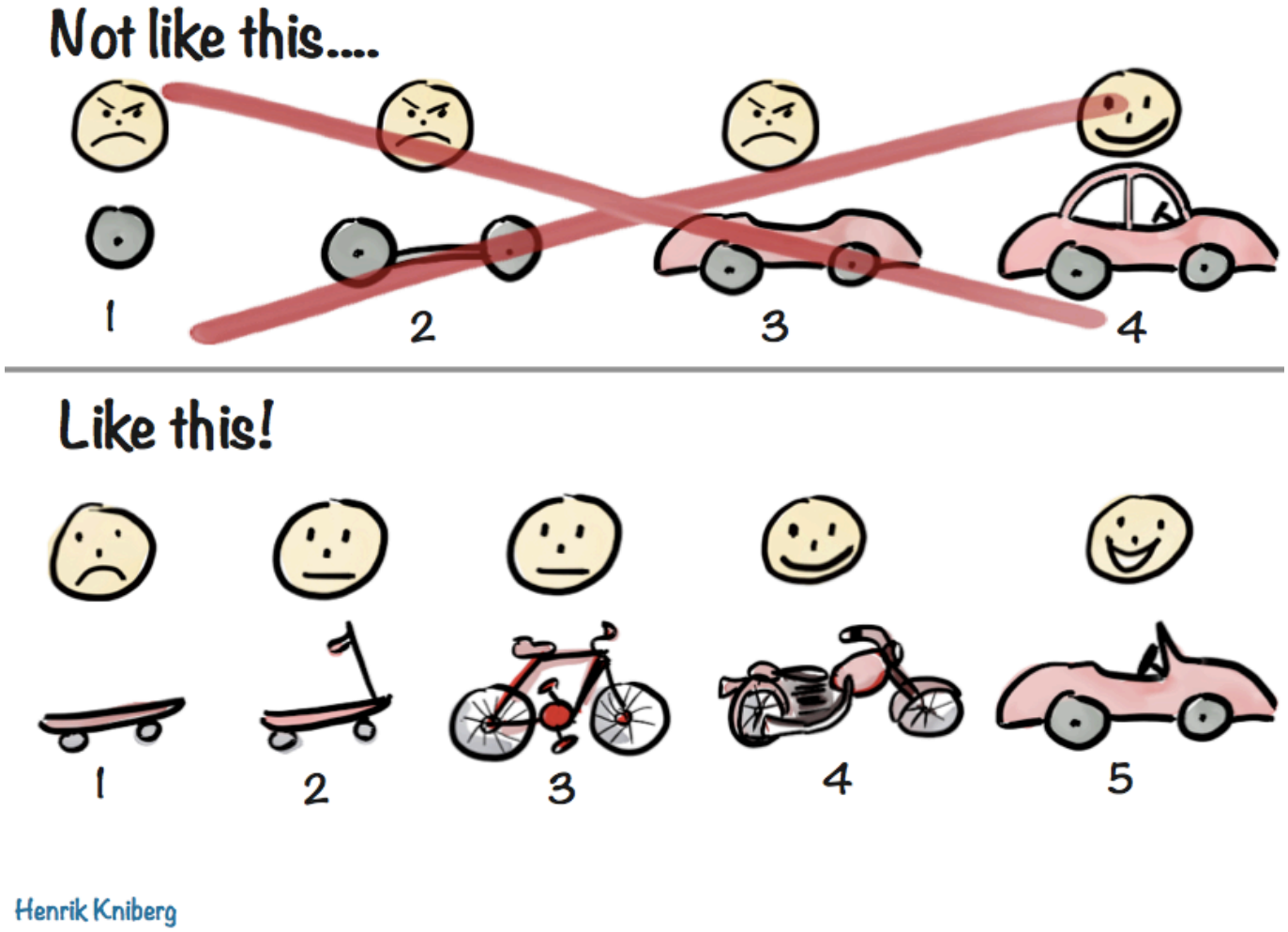
IT Risk management for cloud services (a very simple example)

Event	SLE ("1-5")	ARO ("1-3")	ALE
VM escape	n	m	n x m
Compromised VM			
Vulnerable VM			
Abuse of ToU			
IaaS Downtime			
Compromise of IaaS infrastructure			
Loss of VM data			
Major fault affecting all/most VM's			

IT Risk management for data services (a very simple example)

Event	SLE (“1-5”)	ARO (“1-3”)	ALE
Loss of user data	n	m	n x m
ACLs compromised			
Classification mismatch			
Sensitive information leak			
Compliance issue with sensitive data			
Major performance issue			
Malicious data integrity incident			
Lost of data integrity due a fault or mismanagement			

Suggestions for practical improvements at your site



http://blog.crisp.se/2016/01/25/henrikkniberg/making-sense-of-mvp

Could we do something together?

- Sharing risk registers
- Sharing detailed risks under NDA
- Collecting risk metrics
- Sharing best practices in risk management on a more advance level
- Peer reviews of risk management
- Assessing compliance aspects of risk management