Impacts and Controls

Information Security

Dr Hans Georg Schaathun

Høgskolen i Ålesund

Autumn 2011 – Week 6

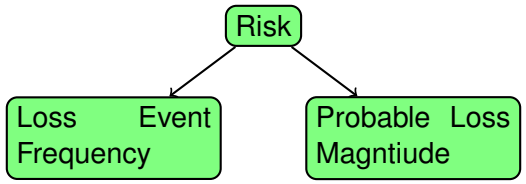
Learning Outcomes

After this week, students should

- be able to complete a simple risk analysis using the FAIR framework.
- know the differences between different types of controls
- have an overview of available controls

Recap – Risk

Risk is potential event which, if occuring, will cause some impact.



Last week, you learnt to assess loss event frequency; now we turn to probable loss magnitude.

This is not easy

- Value of asset cannot easily be determined
- An asset has more than one value/liability characteristic
- Many forms of loss
- Single event needs to multiple types of loss
- Complex systemic relation ship between losses
- Many factors influence loss magnitude

Forms of loss

Productivity reduced abiltity to generate value

Response cost of managing recovery from the impact

Replacement raw cost of replacing an asset

Fines and judgments costs resulting from legal action against the organisation

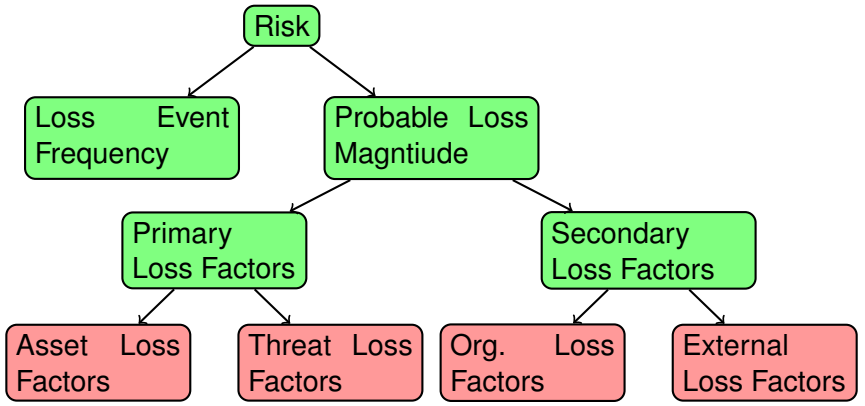
Competitive advantage reduced ability to compete in the market (often associated with loss of trade secrets)

Reputation losses resulting from change in the external perception of the organisation

Loss is assessed from one perspective.

Loss faced by a customer is not relevant, but any resulting loss in reputation or by legal action is relevant.

Loss factors



Loss Factors Explained

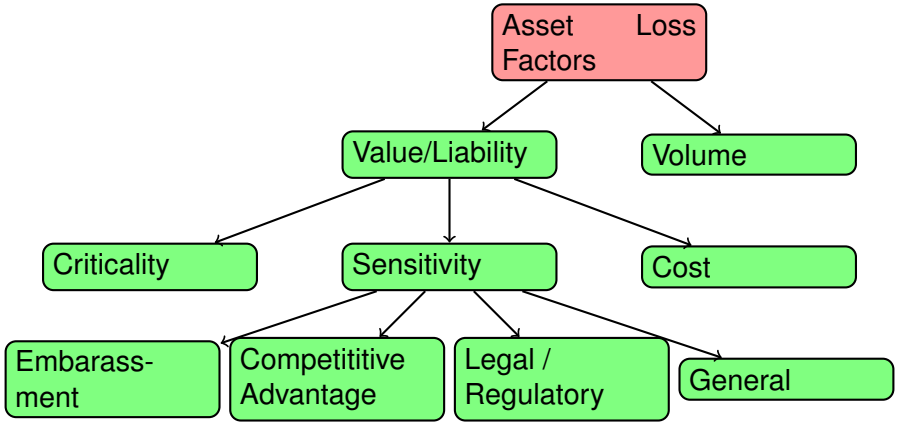
Asset loss factors concerned with the magnitude of the loss

Threat loss factors concerned with how the loss happens

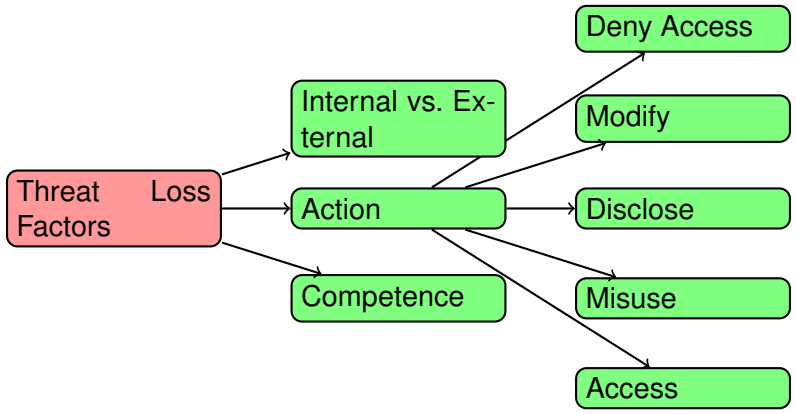
Organisational loss factors refers to controls and vulnerability of the organisation, where they are relevant to loss magnitude

External loss factors

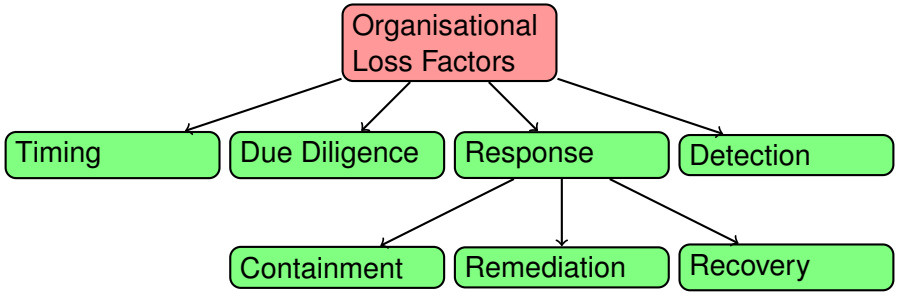
Asset Loss Factors



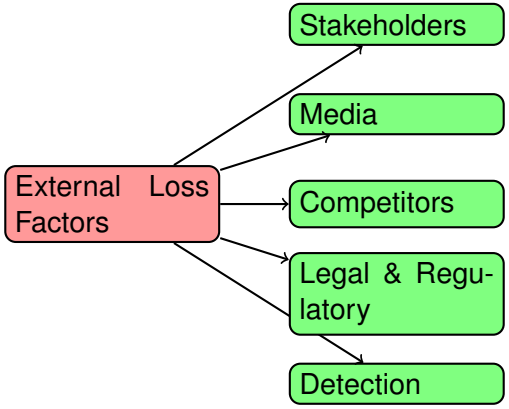
Threat Loss Factors



Organisational Loss Factors



External Loss Factors



Worst-Case Loss

Decision makers tend to want to know the worst case

1. Identify the threat action most likely to result in worst-case loss
2. Estimate magnitude of each loss form
3. Add the loss form magnitudes

Loss Magnitudes

Severe	$\$ 10^7+$
High	$\$ 10^6+$
Significant	$\$ 10^5+$
Moderate	$\$ 10^4+$
Low	$\$ 1,000+$
Very low	$\$ < 1,000$

Probable Loss

- Similar process as worst-case loss
- but cover all plausible threats

Deriving Risk

		Loss Event Frequency				
		VL	L	M	H	VH
PLM	Severe	High	High	Crit	Crit	Crit
	High	Med	High	High	Crit	Crit
	Significant	Med	Med	High	High	Crit
	Moderate	Low	Med	Med	High	High
	Low	Low	Low	Med	Med	Med
	Very low	Low	Low	Med	Med	Med

- The labels are useful to highlight risks which require scrutiny
- *insufficient* for management
  - need to know LEF and PLM too

Døme

Bybanen i Bergen

	Estimert	**Registrert**
Ingen skade	46,4 i året	registeres ikke
Lett skade - førstehjelp	21,6 i året	1
Lett skade - medisinsk behandling	9,3 i året	
Varig skade	$1\frac{1}{2}$ i året	
Alvorlig skade - fare for 1 dødsfall	hvert 19. år	
Dødsfall - 2-10 drepte	hvert 500. år	
Dødsfall - Mer enn 10 drepte	hvert 28.000. år	

Kjelde: `http://www.bt.no/`

Three main classes of Controls

- Technical
- Operational
- Managerial

Technical Controls

What do you think of as technical controls?

- Access Controls
- Audit and Accountability
- Identification and Authentication
- Systems and Communications Protection

Controls primarily implemented in the system (automated).

Operational Controls

- Awareness and Training
- Configuration Management
- Contingency Planning
- Incident Response
- Maintenance
- Media Protection
- Physical and Environmental Protection
- Personnel Security
- System and Information Integrity

Controls primarily implemented by humans.

Management

- Certification, Accreditation, and Security Assessment
- Planning
- Risk Assessment
- System and Services Acquisition

High-level and policy level controls

Security Control Baselines

- Minimum standards for different classes of information
  - in a sense, corresponding to classification levels
- Relative to categorisation according to FIPS 199
  - low-, moderate-, and high-impact
- Higher baselines may require control enhancements

Control Assurance

Low baseline in effect – no obvious vulnerabilities

Moderate baseline documentation and assigned responsibilities – enables testing and auditing

High baseline
- continuity and consistency,
- documentation of design/implementation,
- support for improvement

How difficult is security?

- Which is the most challenging?
  - Building a secure system?
  - Securing a built system?
- Why?

Patchwork security

- Security added as an afterthought.
- Existing, insecure system is extremely complex.
- Reverse-engineering to find flaws.
- Many flaws found only upon attack.
  - Security experts on their heels
  - Patching holes as they are exploited
- System too complex to understand
  - Trial-and-Error

Secure design

- No features ⇒ no security holes.
- Add only secure features.
- Default is always ‘access denied’.
  - Access given when demonstrateably necessary.
  - *Need-to-know* policy
- Security is maintained during the design and building.

Adding features to the box

- Feature-oriented design
  - Users must be able to add data
- Security-oriented design
  - Authorised users and nobody else must be able to add data.
- We only add features if we can maintain security

Question

If it is that simple, why are there so many security issues?

- Security was not prioritised when the system was built.
  - Now, it is a priority
  - Too expensive to rebuild from scratch
- Most developers are not trained for security

KISS

Keep it simple, stupid

What can we learn from the ideal design approach?
When the task is to secure an existing, complex system?

- Consider simple components first
  - asset by asset – how can they be accessed?
  - interface by interface – how can they be (ab)used?
  - user by user – what can they do?
- Analyse the composite sybsystems ...
  - when you understand the components fully

Throughout the module, look for ways to break the system or problem into smaller, simpler pieces.

ACCESS CONTROL POLICY AND PROCEDURES

AC-1 (Technical)

Control: The organization develops, disseminates, and periodically reviews/updates: (i) aformal, documented, access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the access control policy and associated access controls.
Supplemental Guidance: The access control policy and procedures are consistent with applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance. The access control policy can be included as part of the general information security policy for the organization. Access control procedures can be developed for the security program in general, and for a particular information system, when required. NIST Special Publication 800-12 provides guidance on security policies and procedures.
Control Enhancements: None.

Separation of Duties

AC-5 (Technical)

Control: The information system enforces separation of duties through assigned access authorizations.
Supplemental Guidance: The organization establishes appropriate divisions of responsibility and separates duties as needed to eliminate conflicts of interest in the responsibilities and duties of individuals. There is access control software on the information system that prevents users from having all of the necessary authority or information access to perform fraudulent activity without collusion. Examples of separation of duties include: (i) mission functions and distinct information system support functions are divided among different individuals/roles; (ii) different individuals perform information system support functions (e.g., system management, systems programming, quality assurance/testing, configuration management, and network security); and (iii) security personnel who administer access control functions do not administer audit functions.
Control Enhancements: None.

Security Awareness

AT-2 (Operational)

Control: The organization provides basic security awareness training to all information system users (including managers and senior executives) before authorizing access to the system, when required by system changes, and [Assignment: organization-defined frequency, at least annually] thereafter.
Supplemental Guidance: The organization determines the appropriate content of security awareness training based on the specific requirements of the organization and the information systems to which personnel have authorized access. The organization's security awareness program is consistent with the requirements contained in C.F.R. Part 5 Subpart C (5 C.F.R 930.301) and with the guidance in NIST Special Publication 800-50.
Control Enhancements: None.

Time Stamps

AU-8 (Technical)

Control: The information system provides timestamps for use in audit record generation.
Supplemental Guidance: Timestamps (including date and time) of audit records are generated using internal system clocks.
Control Enhancements: (1) The organization synchronizes internal information system clocks [Assignment: organization- defined frequency].
LOW Not Selected – MOD AU-6 (2) – HIGH AU-6 (1) (2)

Information System Connections

CA-3 (Management)

Control: The organization authorizes all connections from the information system to other information systems outside of the accreditation boundary through the use of system connection agreements and monitors/controls the system connections on an ongoing basis.
Supplemental Guidance: Since FIPS199 security categorizations apply to individual information systems, the organization carefully considers the risks that may be introduced when systems are connected to other information systems with different security requirements and security controls, both within the organization and external to the organization. Risk considerations also include information systems sharing the same networks. NIST Special Publication 800-47 provides guidance on connecting information systems. Related security controls: SC-7, SA-9.
Control Enhancements:

Information System Backup

CP-9 (Operational)

Control: The organization conducts backups of user-level and system-level information (including system state information) contained in the information system [Assignment: organization-defined frequency] and protects backup information at the storage location.
Supplemental Guidance: The frequency of information system backups and the transfer rate of backup information to alternate storage sites (if so designated) are consistent with the organization's recovery time objectives and recovery point objectives. While integrity and availability are the primary concerns for system backup information, protecting backup information from unauthorized disclosure is also an important consideration depending on the type of information residing on the backup media and the FIPS 199 impact level. An organizational assessment of risk guides the use of encryption for backup information. The protection of system backup information while in transit is beyond the scope of this control. Related security controls: MP-4, MP-5.

Information System Backup

Control Enhancements

Control Enhancements:

1. The organization tests backup information [Assignment: organization-defined frequency] to verify media reliability and information integrity.
2. The organization selectively uses backup information in the restoration of information system functions as part of contingency plan testing.
3. The organization stores backup copies of the operating system and other critical information system software in a separate facility or in a fire-rated container that is not collocated with the operational software.
4. The organization protects system backup information from unauthorized modification.

Enhancement Supplemental Guidance: The organization employs appropriate mechanisms (e.g., digital signatures, cryptographic hashes) to protect the integrity of information system backups. Protecting the confidentiality of system backup information is beyond the scope of this control. Related security controls: MP-4, MP-5.
LOW CP-9 – MOD CP-9 (1) (4) – HIGH CP-9 (1) (2) (3) (4)

Summary

- Security is compromising
- Compromises
  - functionality and security
  - risk and potential gain
- Security by design is simpler and cheaper
- Refitting controls on a pre-existing system is often necessary