# IN2120 Information Security
# University of Oslo
# Autumn 2019

Lecture 7

Risk Management

Business Continuity Management

UiO, 2019

Audun Jøsang

## What is risk?

- ISO 31000 Risk Management:
  - **"Risk is the effect of uncertainty on objectives"**
  - No distinction between positive and negative effects of uncertainty
  - This definition is very general, and too abstract for IS risk assessment
  - But ISO 31000 also says: **Risk is often expressed as the combination of the *likelihood of occurrence of an event* and the associated *consequences of the event*.**
- ISO 27005 (Information Security Risk)
  - **"Risk is the potential that a given threat will exploit vulnerabilities of assets and thereby cause harm to the organization."**
- Harris, CISSP 8th ed.:
  - **"Risk is the likelihood of a threat agent taking advantage of a vulnerability and the resulting business impact."** (Glossary p.1292)

## Risk Categories

Strategic Risk

- Risk related to long-term strategies and plans
  - Disruptive technological development
  - New Competitors in the market
  - Changing laws, regulation and politics
  - Unstable global economy

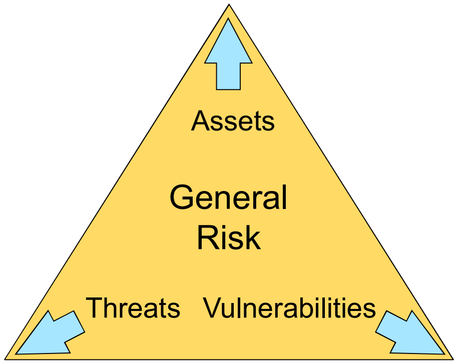
Financial Risk

- Risk related to the financial situation of the organisation
  - Return on investments
  - Sales and price levels in the market
  - Cost of operations
  - Liquidity

Operational Risk

- Risk related to events with negative impact on operations
  - Accidents and failures
  - Natural events (flood, fire)
  - Intentional adversarial actions
  - Information security and cyber incidents

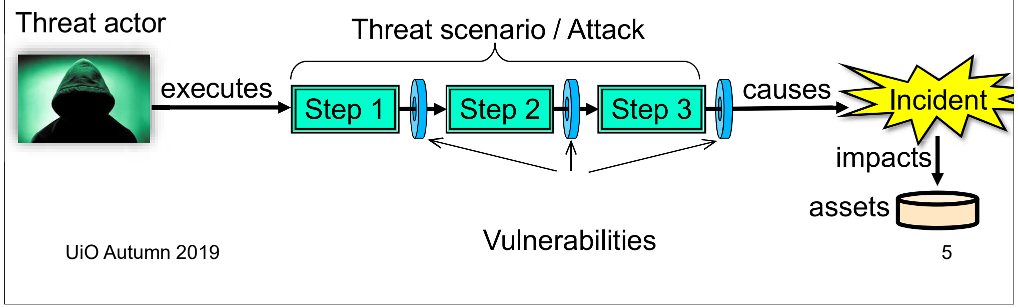
## General IS Risk Model (NSM)



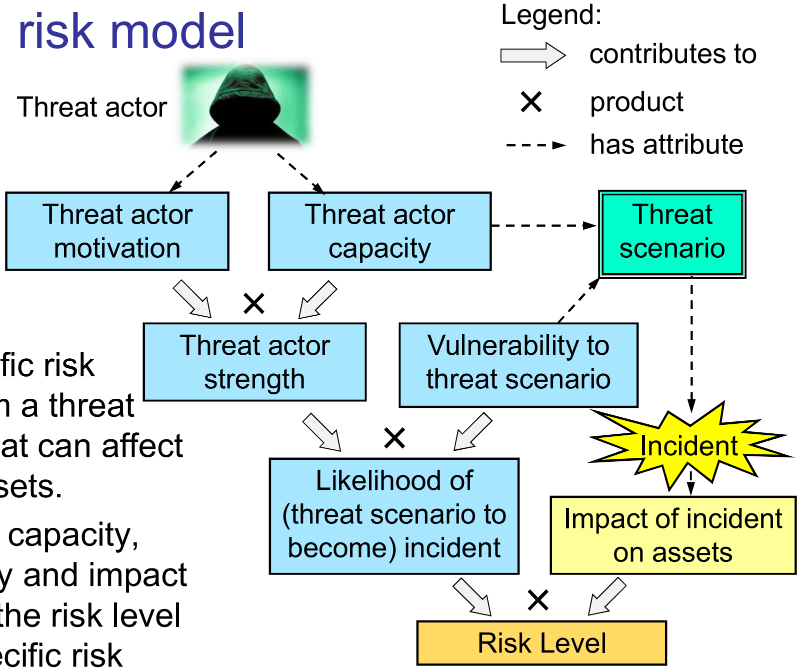
- General model for information-security risk
  - The more assets you have, the more threats you are exposed to, and the more vulnerable you are, then the greater the risk.

# Assets, Threats and Vulnerabilities

- **Asset:** Something which is of value to the organization.
  - The CIA properties of concrete assets, e.g. servers and equipment
  - The CIA and privacy properties of data
- **Threat:** A scenario of steps or procedures, controlled or triggered by a threat actor, which can negatively affect the victim's information assets.
- **Vulnerability:** The absence of security controls to stop a threat scenario.

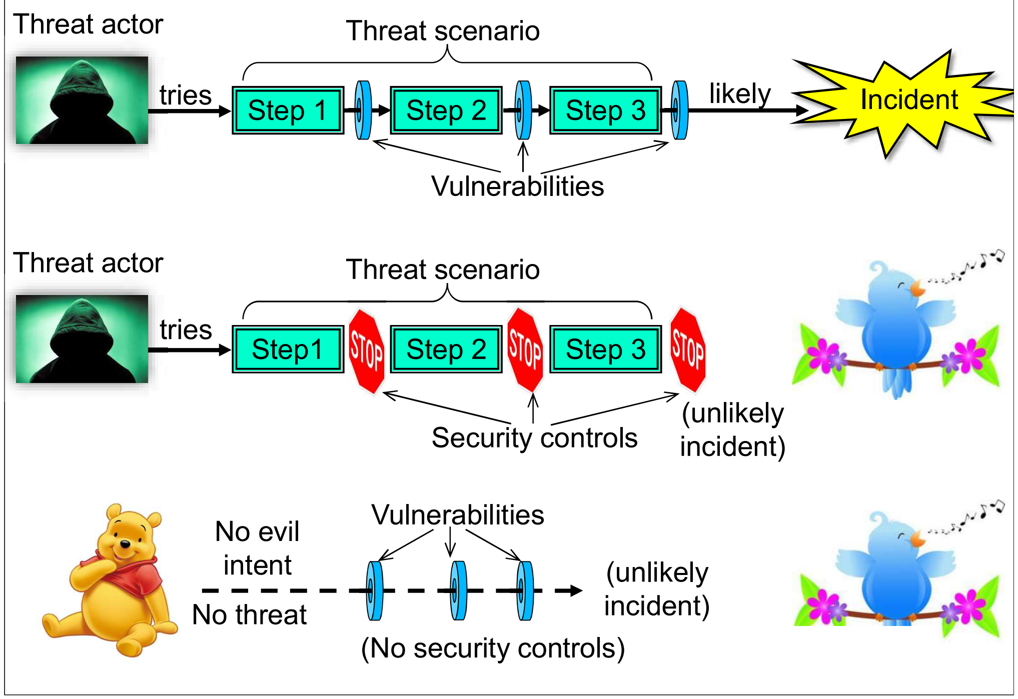


# Detailed risk model



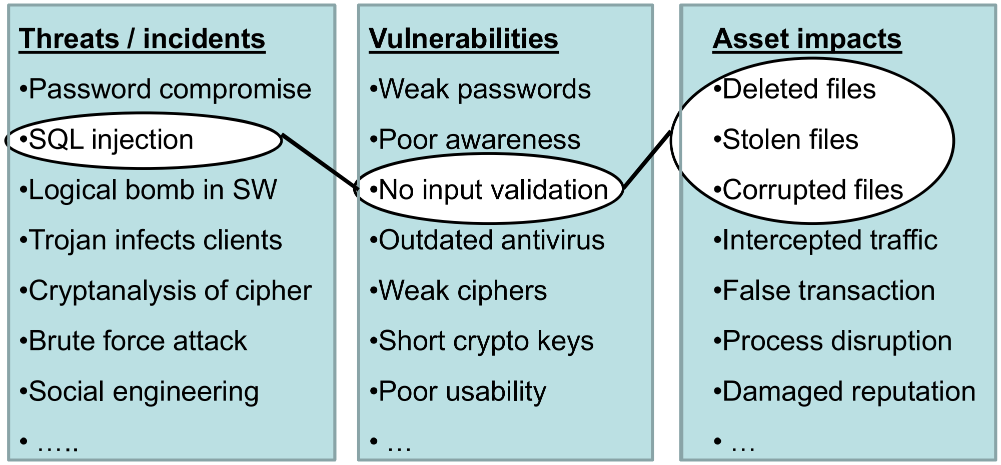
- Each specific risk results from a threat scenario that can affect specific assets.
- Motivation, capacity, vulnerability and impact determine the risk level for that specific risk

# Likelihood of a security incident



# Identifying specific risks

- The relevant combination of a threat scenario, vulnerabilities, and the resulting incident and impact represents a single specific risk
- All relevant specific risks should be identified



**Threats / incidents**

- Password compromise
- SQL injection
- Logical bomb in SW
- Trojan infects clients
- Cryptanalysis of cipher
- Brute force attack
- Social engineering
- …..

**Vulnerabilities**

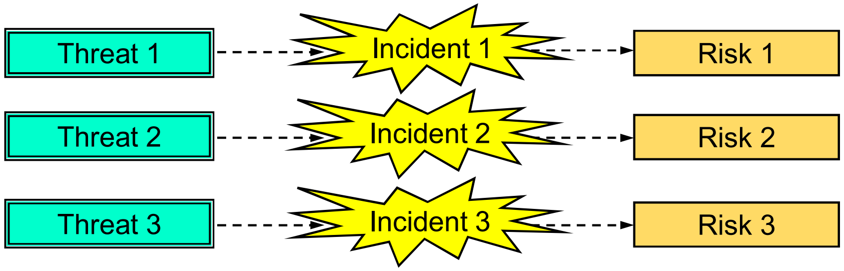
- Weak passwords
- Poor awareness
- No input validation
- Outdated antivirus
- Weak ciphers
- Short crypto keys
- Poor usability
- …

**Asset impacts**

- Deleted files
- Stolen files
- Corrupted files
- Intercepted traffic
- False transaction
- Process disruption
- Damaged reputation
- …

# Many Risks

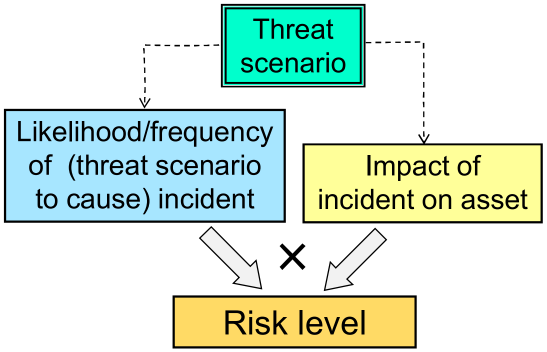
- Multiple different threats (scenarios) can be identified
- Each threat can potentially cause a (different) incident
- Each potential incident has a risk level
- Multiple threats ⇒ Many risks



Threat 1
Incident 1
Risk 1
Threat 2
Incident 2
Risk 2
Threat 3
Incident 3
Risk 3

# The level of a specific risk

- Practical risk analysis typically considers two factors to determine the level of each risk
  1. Likelihood / frequency of each type of incident
  2. Impact on assets (loss) resulting from each type of incident



Threat scenario
Likelihood/frequency of (threat scenario to cause) incident
Impact of incident on asset
×
Risk level

# Risk Management standards

- ISO 31000 Risk Management
- ISO 27005 Information Security Risk Management
- NIST SP800-39 Managing Information Security Risk
- NIST SP800-30 Guide for Conducting Risk Assessment
  - formerly called “Risk Management Guide for Information Technology Systems”
- NS 5831 Samfunnssikkerhet – Beskyttelse mot tilsiktede uønskede handlinger –Risikohåndtering
- NS 5832 Samfunnssikkerhet – Beskyttelse mot tilsiktede uønskede handlinger – Risikoanalyse

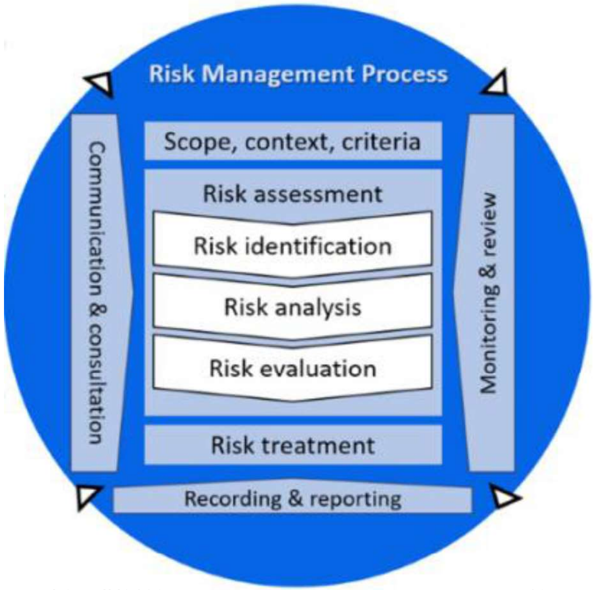
# What is risk management?

- “Risk management consists of coordinated activities to direct and control an organization with regard to risk.”
  - ISO 31000

- “IS risk management analyses what can happen and what the possible consequences can be, before deciding what should be done and when, to reduce risk to an acceptable level.”
  - ISO 27005

# Risk Management Process: ISO 31000

- ISO 31000 is a general standard for risk management applicable to different sectors
- The same approach is applicable to IS risk management



Risk Management Process

Communication & consultation

Scope, context, criteria

Risk assessment

Risk identification

Risk analysis

Risk evaluation

Risk treatment

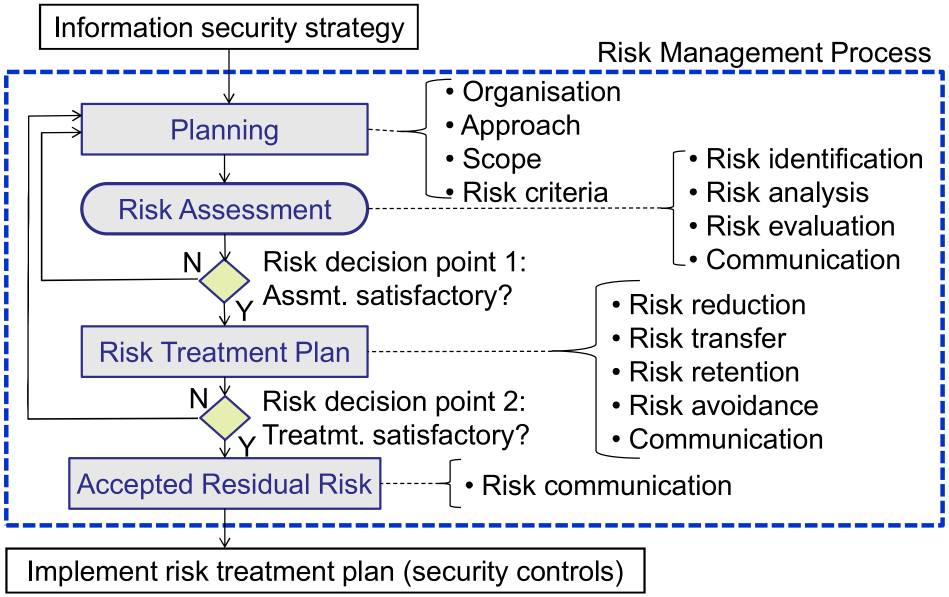
Monitoring & review

Recording & reporting

# Basis for assessing risk

- Know the assets: identify and understand the value of information assets and systems.
- Know the threats: identify and understand relevant threat scenarios which can harm information assets and systems.
- Know the vulnerabilities which can be exploited by threats.
- Know the potential impacts of incidents.
- Know which stakeholders in the organisation are responsible for managing the identified risks.

# Risk management process ISO 27005



Information security strategy

Risk Management Process

Planning

- Organisation
- Approach
- Scope
- Risk criteria

Risk Assessment

- Risk identification
- Risk analysis
- Risk evaluation
- Communication

N Risk decision point 1: Assmt. satisfactory? Y

Risk Treatment Plan

- Risk reduction
- Risk transfer
- Risk retention
- Risk avoidance
- Communication

N Risk decision point 2: Treatmt. satisfactory? Y

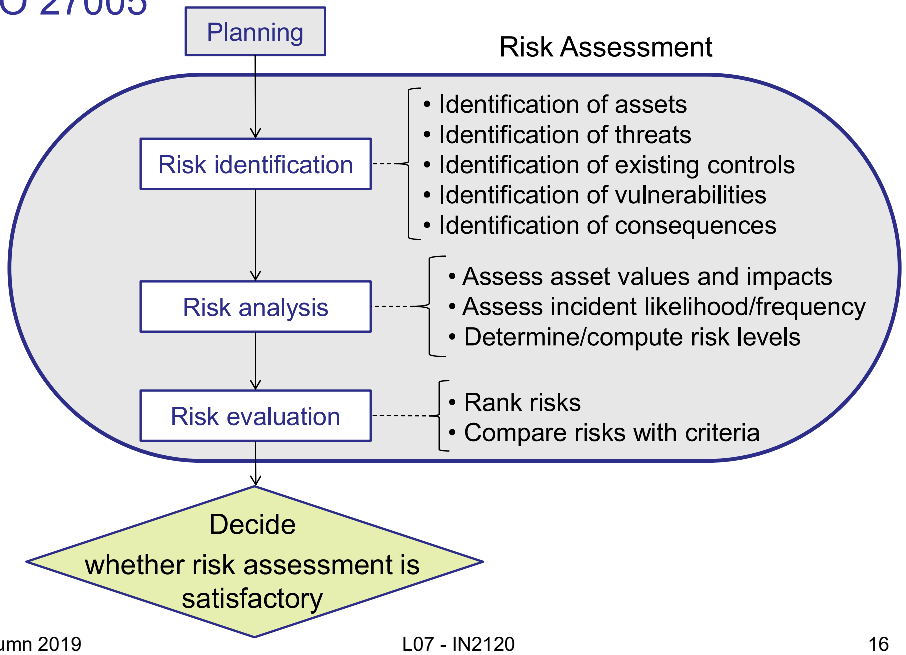
Accepted Residual Risk

- Risk communication

Implement risk treatment plan (security controls)

# Risk assessment process

## ISO 27005



Planning

Risk Assessment

Risk identification

- Identification of assets
- Identification of threats
- Identification of existing controls
- Identification of vulnerabilities
- Identification of consequences

Risk analysis

- Assess asset values and impacts
- Assess incident likelihood/frequency
- Determine/compute risk levels

Risk evaluation

- Rank risks
- Compare risks with criteria

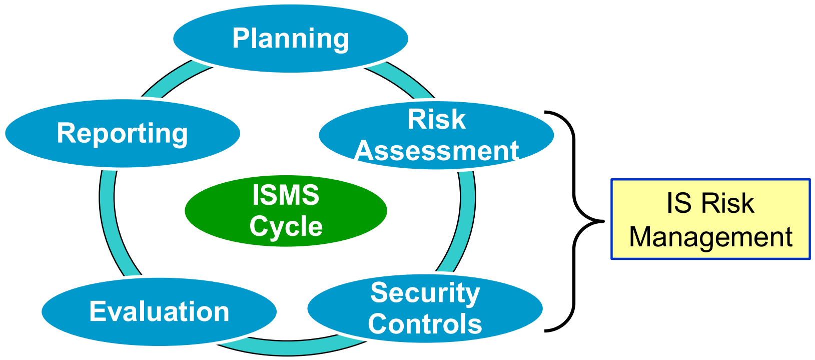
Decide whether risk assessment is satisfactory

# Roles involved in risk management

- Management, users, and information technology must all work together
  - Asset owners must participate in developing asset inventory
  - Users and experts must assist in identifying threats and vulnerabilities, and in determining likelihoods of incidents
  - Risk management experts must guide stakeholders through the risk assessment process
  - Security experts must assist in selecting security controls
  - Management must review the risk management process and approve risk management strategy (security controls)

# Risk Management – ISMS integration

- Risk management is an essential element of ISMS
  - Used to identify risks and their magnitude
  - Basis for selecting security controls
  - Tool for top management to understand organization’s risk exposure



# Asset and Impact Valuation

- Identify relevant assets, and define relevant security aspects
- For example, which information assets are the most critical to the organization’s success with regard to the following aspects:
  1. generates the most revenue/profitability?
  2. is the most important for legal compliance (e.g. GDPR)?
  3. would be the most embarrassing if compromised?
- Valuation
  - Estimate impact on assets from the combined set of aspects
  - Example impact level computation using coproduct (“OR” rule),
    - Let $p_1$ denote relative impact on asset aspect 1, with value in [0,1]
    - Coproduct: $\coprod(p_1, p_2) \quad = p_1 \amalg p_2 \quad = p_1 + p_2 - p_1p_2$
    - Coproduct: $\coprod(p_1, p_2, p_3) = p_1 \amalg p_2 \amalg p_3 = (p_1 \amalg p_2) \amalg p_3$ $= p_1 + p_2 + p_3 + p_1p_2p_3 - p_1p_2 - p_1p_3 - p_2p_3$
    - The relative impact levels can be mapped to qualitative levels

# Example Asset and Impact Valuation

| **Information asset (corresponding incident)** | **Aspect 1** Impact on revenue / profit | **Aspect 2** Impact on legal compliance | **Aspect 3** Impact on public image | **Total impact of incidents** (coproduct) |
|---|---|---|---|---|
| System and network availability (unavailability) | 0.9 | 0.0 | 0.2 | 0.92 |
| Product data (loss of) integrity | 0.4 | 0.0 | 0.0 | 0.40 |
| Customer profiles (loss of) integrity | 0.5 | 0.0 | 0.0 | 0.50 |
| Customer profiles (loss of) confidentiality | 0.0 | 0.8 | 0.5 | 0.90 |
| Customer credentials (loss of) confidentiality | 0.9 | 0.0 | 0.4 | 0.94 |
| Web page integrity (defacement) | 0.1 | 0.0 | 0.1 | 0.19 |
| User support (un) availability | 0.2 | 0.0 | 0.1 | 0.28 |

- All values are relative in the interval [0, 1]

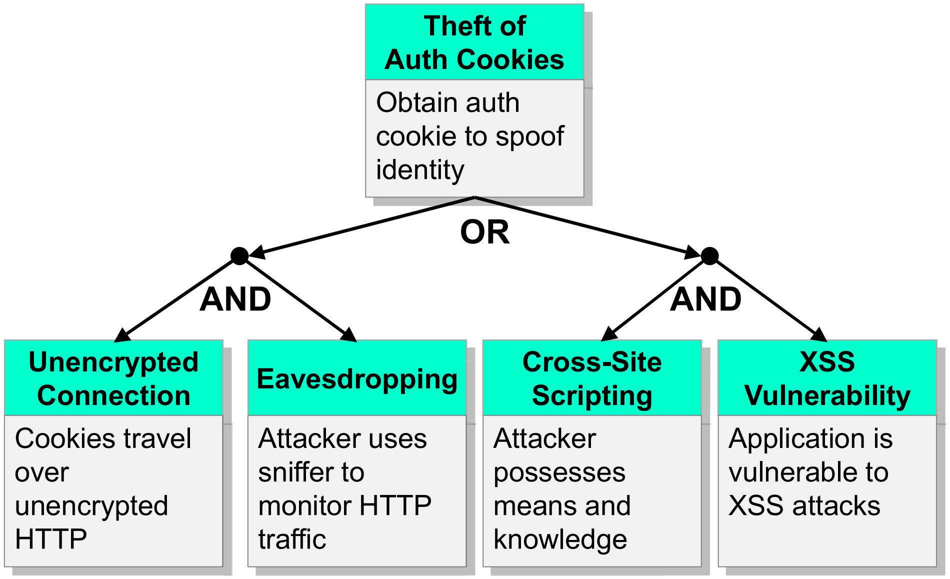
# Threat Modelling

- Threat modelling is the process of identifying, analysing and describing relevant threat scenarios.
- Unimportant/irrelevant threat scenarios can be ignored.
- Examine how each relevant threat scenario can be executed against the organization's assets.
- The threat modelling process works best when people with diverse backgrounds within the organization work together in a series of brainstorming sessions.
- Threat modelling is important during system development
  - Used to identify, remove and avoid vulnerabilities when developing software and systems.
- Multiple approaches/methods for threat modelling

# Threat Modelling Methods

- Attacker-centric
  - Starts from attackers, evaluates their goals, and how they might achieve them through attack tree. Usually starts from entry points or attacker action.
- System-centric (aka. SW-, design-, architecture-centric)
  - Starts from model of system, and attempts to follow model dynamics and logic, looking for types of attacks against each element of the model. This approach is e.g. used for threat modeling in Microsoft's Security Development Lifecycle.
- Asset-centric
  - Starts from assets entrusted to a system, such as a collection of sensitive personal information, and attempts to identify how security breaches of CIA properties can happen.

# Attacker Centric: Threat Tree Example



**Theft of Auth Cookies**
Obtain auth cookie to spoof identity

OR

AND

**Unencrypted Connection**
Cookies travel over unencrypted HTTP

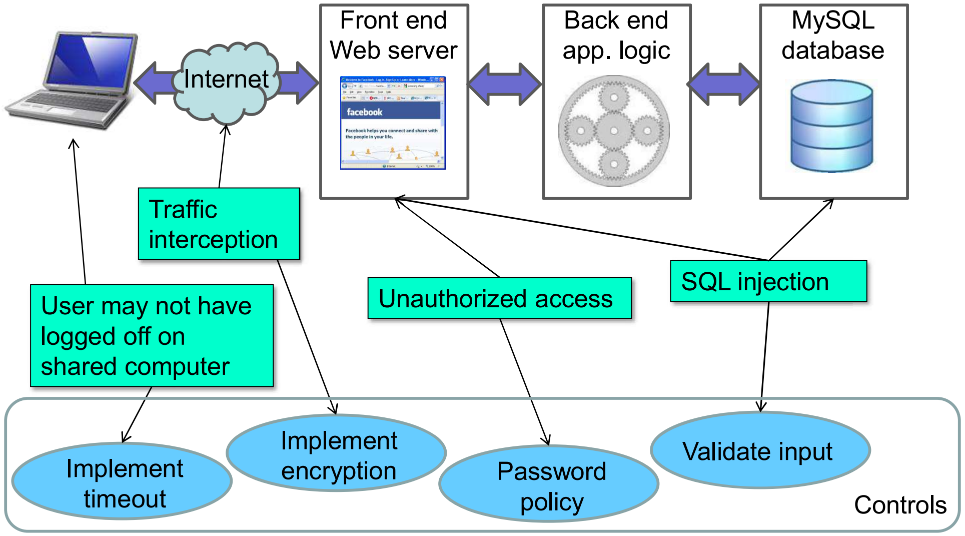
**Eavesdropping**
Attacker uses sniffer to monitor HTTP traffic

AND

**Cross-Site Scripting**
Attacker possesses means and knowledge

**XSS Vulnerability**
Application is vulnerable to XSS attacks

# System-centric threat modelling example



Traffic interception

User may not have logged off on shared computer

Unauthorized access

SQL injection

Implement timeout

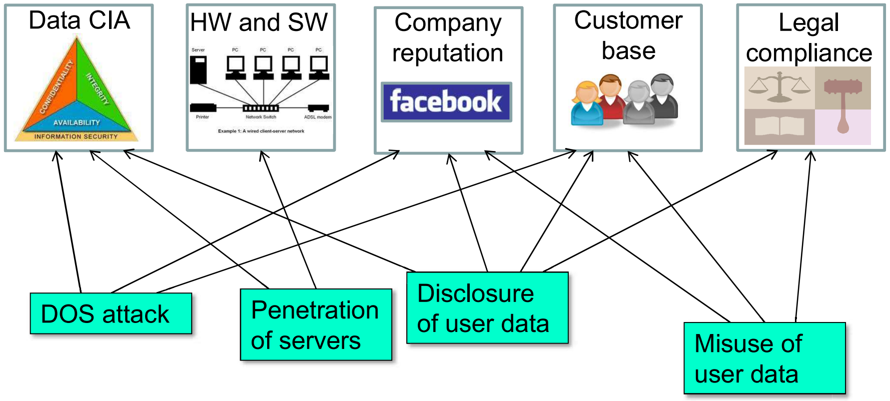
Implement encryption

Password policy

Validate input

Controls

## Asset-centric threat modelling example



## Vulnerability Identification

- Vulnerabilities are specific opportunities that threat actors can exploit to attack systems and information assets.
- Generic vulnerability identification
  - To identify a vulnerability is the same as to determine how to block a specific threat scenario.
  - Removing a vulnerability is the same as blocking a threat.
  - A vulnerability is **the absence of barriers** against a threat.
  - Blocking a threat (i.e. removing a vulnerability) is done with a security control.
- Tool-based and checklist-based vulnerability identification
  - **Vulnerability scanners** are automated tools to detect known vulnerabilities in networks and systems, e.g. Wireshark
  - **Check lists of vulnerabilities** are used by teams when doing risk assessment and removing vulnerabilities, e.g. OWASP Top 10.

## No vulnerability without a threat

Karl Johan Street
Oslo

New terrorist threat appears in 2016

Nice
Berlin
London
Barcelona

Threat blocked and vulnerability removed

## Feilbetegnelsen “ROS-analyse”

- ROS-analyse = «Risiko- og sårbarhetsanalyse»
- Begrepet «sårbarhet» som del av ROS-analyse betyr «kombinasjonen av sannsynlighet for en hendelse og dens konsekvens», som egentlig er det samme som risiko.
- Denne definisjonen av «sårbarhet» stammer fra rapportene til «Sårbarhetsutvalget» i 2000 og «Lysneutvalget» i 2015.
- Med denne definisjonen er sårbarhet = risiko, og «sårbarhetsanalyse» blir det samme som risikoanalyse.
- Begrepet ROS-analyse brukes ofte på norsk, og er faktisk et særnorsk begrep.
- Begrepet ROS-analyse og dens definisjon på «sårbarhet» kan skape forvirring, og bør unngås.

# Estimating risk levels

Types of analysis

- **Qualitative**
  - Uses descriptive scales. Example:
    - Impact level: Minor, moderate, major, catastrophic
    - Likelihood: Rare, unlikely, possible, likely, almost certain
- **Relative**
  - Relative numerical values assigned to qualitative scales
  - Gives relatively good distribution of risk levels
- **Quantitative**
  - Use numerical values for both consequence (e.g. $) and likelihood (e.g. probability value)

# Qualitative likelihood scale

Increasing Likelihood

| **Likelihood** | **Description** |
|---|---|
| High | Is expected to occur in most conditions (1 or more times per year). |
| Medium | The event will probably happen in most conditions (every 2 years). |
| Low | The event should happen at some time (every 5 years). |
| Unlikely | The event could happen at some time (every 10 years). |

# Qualitative impact level scale

Increasing Impact

| **Impact Level** | **Description** |
|---|---|
| Major | **Major problems** would occur and threaten the provision of important processes **resulting in significant financial loss**. |
| Moderate | **Services would continue**, but would **need to be reviewed or changed.** |
| Minor | Effectiveness of services would be **threatened but dealt with**. |
| Insignificant | Dealt with as a part of **routine operations**. |

# Qualitative risk estimation - example

- Define a risk matrix with a suitable set of qualitative levels
  - qualitative levels for likelihood, impact and risk
- Use the risk matrix as a look-up table to determine the level of each risk

**Qualitative impact levels**

**Qualitative likelihood**

| Risk levels | Insignificant | Minor | Moderate | Major |
|---|---|---|---|---|
| High | M | H | VH | E |
| Medium | L | M | H | VH |
| Low | VL | L | M | H |
| Unlikely | N | VL | L | M |

Legend
**E: extreme risk**; Risk must be handled with priority
**(V)H: (very) high risk**; Risk must be handled
**M: moderate risk**; Risk to be handled according to budget
**(V)L: (very) low risk**; Risk with low priority, handle if there is opportunity
**N: Negligible risk;** To be ignored

# Relative risk estimation
## Example

**Relative risk levels:** Product of likelihood & impact level

**Relative Impact levels**

**Relative likelihood levels**

| Relative risk levels | (0.0) Nil | (0.1) Insign. | (0.2) Minor | (0.4) Moderate | (1.0) Major |
|---|---|---|---|---|---|
| (1.0) High | 0 | 0.10 | 0.20 | 0.40 | 1.00 |
| (0.4) Medium | 0 | 0.04 | 0.08 | 0.16 | 0.40 |
| (0.2) Low | 0 | 0.02 | 0.04 | 0.08 | 0.20 |
| (0.1) Unlikely | 0 | 0.01 | 0.02 | 0.04 | 0.10 |
| (0.0) Never | 0 | 0 | 0 | 0 | 0 |

Relative risk estimation can give a better distribution of risk levels than with purely qualitative models.

# Quantitative risk estimation example

Example quantitative risk analysis method

- Quantitative parameters
  - Asset Value (AV)
    - Estimated total value of asset
  - Exposure Factor (EF)
    - Percentage of asset loss caused by threat occurrence
  - Single Loss Expectancy (SLE)
    - SLE = AV × EF
  - Annualized Rate of Occurrence (ARO)
    - Estimated frequency a threat will occur within a year
  - Annualised Loss Expectancy (ALE)
    - ALE = SLE × ARO

# Quantitative risk estimation example

## Example quantitative risk analysis

- Risk description
  - Asset: Public image (and trust)
  - Threat: Defacing web site through intrusion
  - Impact: Loss of image
- Parameter estimates
  - AV(public image) = $1,000,000
  - EF(public image affected by defacing) = 0.05
  - SLE = AV × EF = $50,000
  - ARO(defacing) = 2
  - ALE = SLE × ARO = $100,000

- Justifies spending up to $100,000 p.a. on controls

# Risk listing and ranking

| **Threat scenario:** | **Existing controls & vulnerabilities:** | **Asset impact:** | **Impact level:** | **Likelihood description:** | **Likelihood:** | **Risk level:** |
|---|---|---|---|---|---|---|
| Compromise of user password | No control or enforcement of password strength | Deleted files, breach of confidentiality and integrity | MODE RATE | Will happen to 1 of 50 users every year | MEDIUM | HIGH |
| Virus infection on clients | Virus filter disabled on many clients | Compromise of clients | MODE RATE | Will happen to 1 in 100 clients every year | HIGH | EXTREME |
| Web server hacking and defacing | IDS, firewall, daily patching, but zero day exploits exist | Reputation | MINOR | Could happen once every year | MEDIUM | MODE RATE |
| Logical bomb planted by insider | No review of source code that goes into production. | Breach of integrity or loss of data | MAJOR | Could happen once every 10 years | UNLIKELY | MODE RATE |

## Problems of measuring risk

Businesses normally wish to measure risk in money, but almost impossible to do this

- Valuation of assets
  - Value of data, hard to assess
  - Value of goodwill and customer confidence, very vague
- Likelihood of incidents
  - Past events not always relevant for future probabilities
    - The nature of future attacks is unpredictable
    - The actions of future attackers are unpredictable
- Measurement of benefit from security control
  - Problems with the difference of two approximate quantities
    - Estimation of past and present risk

## Risk Control Strategies

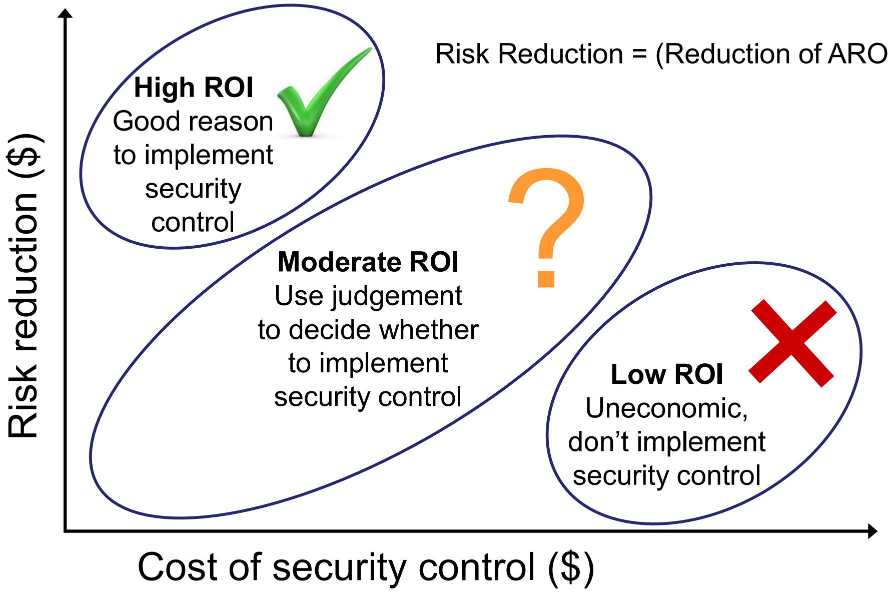
- After completing the risk assessment, the security team must choose one of four strategies to control each risk:

1. Reduce risk by implementing security controls
2. Share/transfer risk (outsource activity that causes risk, or buy insurance)
3. Retain risk (understand and tolerate potential consequences)
4. Avoid risk (stop activity that causes risk)

## ROI of Security Controls (Return on Investment)

$$\text{Security Control ROI} = \frac{\text{Risk Reduction – Cost of Control}}{\text{Cost of Control}}$$

Risk Reduction = (Reduction of ARO) * SLE



**High ROI** Good reason to implement security control

**Moderate ROI** Use judgement to decide whether to implement security control

**Low ROI** Uneconomic, don't implement security control

## Business Continuity Management

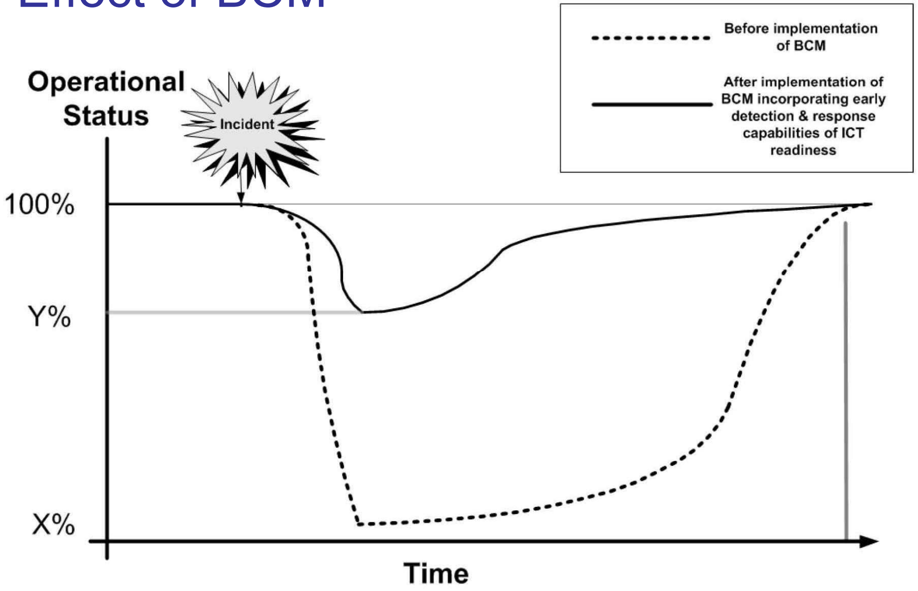
Outline

- Business Continuity Planning
- Business Impact Analysis

# Business Continuity Management

- Procedures for the recovery of an organization's facilities in case of major incidents and disasters, so that the organization will be able to either maintain or quickly resume mission-critical functions
- BCM standards
  - ISO 27031 Guidelines for ICT readiness for business continuity
  - NISTSP800-34 Contingency Planning Guide for Federal Information Systems

# Effect of BCM



# Business continuity management

- The range of incidents and disasters to be considered include:
  - Acts of nature, for example:
    - Excessive weather conditions
    - Earthquake
    - Flood
    - Fire
  - Human acts (inadvertent or deliberate), for example:
    - Hacker activity
    - Mistakes by operating staff
    - Theft
    - Fraud
    - Vandalism
    - Terrorism

# Business Continuity Plan (BCP)

From:

Getting control over the crisis

To:

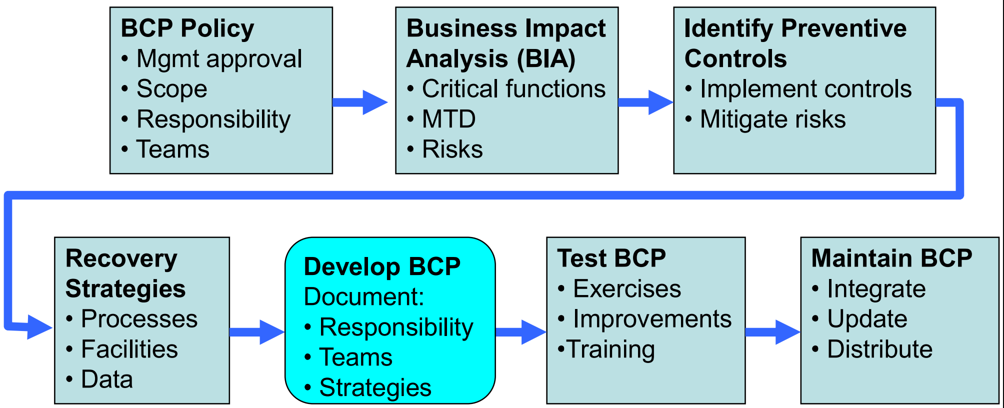
Back in business

- The business continuity plan describes:
  - a sequence of actions
  - and the parties responsible for carrying them out
  - in response to disasters
  - in order to restore normal business operations as quickly as possible

# BCP Terminology

- Business Continuity Plan
  - Plan for restoring normal business functions after disruption
- Business Contingency Plan
  - Same as Business Continuity Plan
  - Contingency means ”something unpredictable that can happen”
- Disaster Recovery
  - Reestablishment of business functions after a disaster, possibly in temporary facilities
  - Requires a BCP
- Business Continuity Management
  - Denotes the management of Business Continuity
  - Includes the establishment of a BCP
  - ICT Readiness for Business Continuity (IRBC) (term used in ISO27031)

# BCP Management (same as IRBC)



**BCP Policy**
- Mgmt approval
- Scope
- Responsibility
- Teams

**Business Impact Analysis (BIA)**
- Critical functions
- MTD
- Risks

**Identify Preventive Controls**
- Implement controls
- Mitigate risks

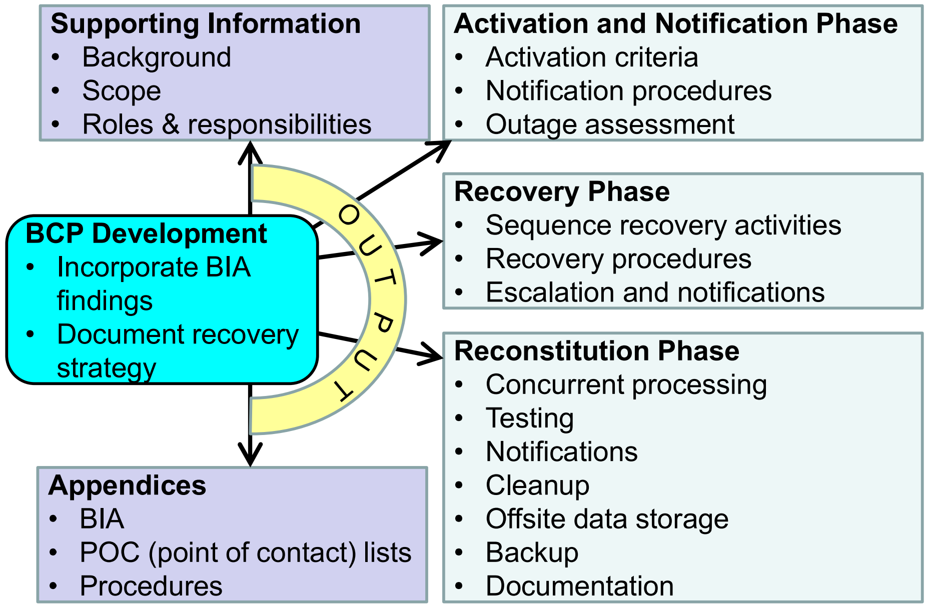
**Recovery Strategies**
- Processes
- Facilities
- Data

**Develop BCP** Document:
- Responsibility
- Teams
- Strategies

**Test BCP**
- Exercises
- Improvements
- Training

**Maintain BCP**
- Integrate
- Update
- Distribute

Source: NIST Special Publication 800-34 rev.1
Contingency Planning Guide for Information Technology Systems (p.13)



**Supporting Information**
- Background
- Scope
- Roles & responsibilities

**Activation and Notification Phase**
- Activation criteria
- Notification procedures
- Outage assessment

**BCP Development**
- Incorporate BIA findings
- Document recovery strategy

**Recovery Phase**
- Sequence recovery activities
- Recovery procedures
- Escalation and notifications

**Reconstitution Phase**
- Concurrent processing
- Testing
- Notifications
- Cleanup
- Offsite data storage
- Backup
- Documentation

**Appendices**
- BIA
- POC (point of contact) lists
- Procedures

BCP Development and Output: NIST SP800-34, rev.1 p.34

# BIA: Business Impact Analysis

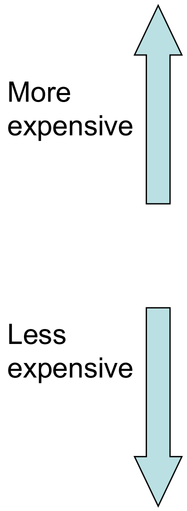
- A Business Impact Analysis (BIA) is performed as part of the BCP development to identify the functions that in the event of a disaster or disruption, would cause the greatest financial or operational loss.
- Consider e.g.:
  - IT network support
  - Data processing
  - Accounting
  - Software development
  - Payroll

  Customer support
  Order entry
  Production scheduling
  Purchasing
  Communications

# BIA (continued)

- The MTD (Maximum Tolerable Downtime) is defined for each function in the event of disaster.
- Example:
  - Non-essential = 30 days
  - Normal = 7 days
  - Important = 72 hours
  - Urgent = 24 hours
  - Critical = minutes to hours

# Alternative Sites



- Redundant site
  - Mirror of the primary processing environment
  - Operable within minutes
- Hot site
  - Fully configured hardware and software, but no data
  - Operable within hours
- Cloud
- Warm site
  - Partially configured with some equipment, but not the actual computers
  - Operable within days
- Cold site
  - Basic electricity and plumbing
  - Operable within weeks

Whenever relevant, consider cloud services, which can be relatively low cost

# BCP Testing

- Checklist test
  - Copies of the BCP distributed to departments for review
- Structured walk-through test
  - Representatives from each department come together to go through the plan
- Simulation test
  - All staff in operational and support functions come together to practice executing the BCP
- Parallel test
  - Business functions tested at alternative site
- Full interruption test
  - Business functions at primary site halted, and migrated to alternative site in accordance with the BCP

End of Lecture