A Computer Warm in 2000

- **An email message**
  - subject line "ILOVEYOU" and
  - attachment "LOVE-LETTER-FOR-YOU.txt.vbs”
- **Opening the attachment**
  - activates the Visual Basic script
    - Overwriting image files,
    - Sent a copy of itself to the first 50 addresses in the Windows Address Book used by Microsoft Outlook
- **Success**
  - Scripting engine is enabled
  - Advantage of Microsoft algorithm to hiding file extensions
  - Social engineering
  - Microsoft design weakness
    - Access to operating systems
    - Secondary storage
- **Impact**
  - Within 10 days
    - 50 million (10% of the Internet connected computers) infections reported
    - Pentagon, CIA, British Parliament made a complete shut down of their mail systems
  - $5.5-8.7 billion damage
  - $15 billion to remove the worm

http://en.wikipedia.org/wiki/ILOVEYOU

Another example

MTAT.03.307

Principles of Secure Software Design

Dr. Raimundas Matulevičius
University of Tartu
email: rma@ut.ee

On successful completion of this course

- Identify causes and consequences of (lack of) system and software security
- Master essential techniques to reduce and avoid system and software security problems, to introduce and reason on security requirements and controls
- Apply advanced modelling techniques (notations, tools, and processes) to build secure systems and software

About the Course

- **Course Website**
  - **https://courses.cs.ut.ee/2017/ssd/spring**
  - **Lectures**
    - Presented during lectures - uploaded to before the lecture
    - Lecture videos – uploaded after the lecture
  - **Practicals**
    - Exercises and Workshops done during the practical sessions
    - Home assignments
  - **Readings**
    - Self-study material
    - Articles and other readings
  - **Upload**
    - Place where you will be able to upload solutions to all home assignments
  - **Grading**
    - Grading modalities explained
  - **Exam**
    - Previous year exams – tasks and some solutions
    - This year exam (tasks will be uploaded after the exam)

About the Course

- **Course Website**
  - **https://courses.cs.ut.ee/2017/ssd/spring**
  - **Lectures**
    - Presented during lectures - uploaded to before the lecture
    - Lecture videos – uploaded after the lecture

Message Board

https://piazza.com/ut.ee/spring2017/mtat03307/home

Fell free to post and discuss the course related questions, or provide feedback.

  - **Grading**
    - Grading modalities explained
  - **Exam**
    - Previous year exams – tasks and some solutions
    - This year exam (tasks will be uploaded after the exam)

Course outline / Schedule

1	Security Risk Management	R. Matulevičius	9 February
2	Security Modelling	R. Matulevičius	16 February
3	Security Modelling	R. Matulevičius	23 February
4	Security Modelling	R. Matulevičius	2 March
5	Security Threats	vičius	9 March
6	Security Require	vičius	16 March
7	RBAC: Role-bas	vičius	23 March
8	Model-driven S	vičius	30 March
9	Introduction to C		6 April
10	Estonian X-Road	enthal	13 April
11	Internet Voting	g	20 April
12	Dependability Requirements	R. Matulevičius	27 April
13	Social Engineering	R. Matulevičius	4 May
14	Security Patterns	R. Matulevičius	11 May
15	Secure Software Processes	R. Matulevičius	18 May

Thursdays

Lectures
- Room **405**, 12:15 – 14:00

Practicals:
- Room **403**, 14:15 – 16:00
- Room **402**, 16:15 – 18:00

Changes are possible!

Course outline / Schedule

1	Security Risk Management	R. Matulevičius	9 February
2	Security Modelling	R. Matulevičius	16 February
3	Security Modelling	R. Matulevičius	23 February
4	Security Modelling	R. Matulevičius	2 March
5	Security Threats, Errors and their types	R. Matulevičius	9 March
6	Security Requirements	R. Matulevičius	16 March
7	RBAC: Role-based Access Control	R. Matulevičius	23 March
8	Model-driven Security: RBAC workshop	R. Matulevičius	30 March
9	Introduction to Cryptography	D.Unruh	6 April
10	Estonian X-Road	M. Freudenthal	13 April
11	Internet Voting	S. Heiberg	20 April
12	Dependability Requirements	R. Matulevičius	27 April
13	Social Engineering	R. Matulevičius	4 May
14	Security Patterns	R. Matulevičius	11 May
15	Secure Software Processes	R. Matulevičius	18 May

Changes are possible!

Course outline / Schedule

1	Security Risk Management	R. Matulevičius	9 February
2	Security Modelling	R. Matulevičius	16 February
3	Security Modelling	R. Matulevičius	23 February
4	Security Modelling	R. Matulevičius	2 March
5	Securit		rch
6	Securit		arch
7	RBAC:		arch
8	Model-		arch
9	Introdu		ril
10	Estonia		pril
11	Interne		pril
12	Depend		pril
13	Social Engineering	R. Matulevičius	4 May
14	Security Patterns	R. Matulevičius	11 May
15	Secure Software Processes	R. Matulevičius	18 May

Minimal attendance requirements

Mandatory lectures:

Lecture 10 (13.April) ***OR*** **Lecture 11 (20.April)**

Mandatory practical:

Practicals 4 (2.March)

Changes are possible!

Course outline / Schedule

1	Security Risk Management	R. Matulevičius	9 February
2	Security Modelling	R. Matulevičius	16 February
3	Security Modelling	R. Matulevičius	23 February
4	Security Modelling	R. Matulevičius	2 March
5	Securit		rch
6	Securit		arch
7	RBAC:		arch
8	Model-		arch
9	Introdu		ril
10	Estonia		pril
11	Interne		pril
12	Depend		pril
13	Social Engineering	R. Matulevičius	4 May
14	Security Patterns	R. Matulevičius	11 May
15	Secure Software Processes	R. Matulevičius	18 May

Minimal attendance requirements

Mandatory exam:

1. June ***OR*** **8.June**

Changes are possible!

Workload

6 ECTS = 156 hours of study
(1 ECTS = 26 hours of study)

- Lectures – **30** hours
- Practicals – **22** hours
- Independent work – **104** hours
  - Self-study (e.g., reading literature)
  - Homework assignments

Modalities and Assessment

- **Practicals** (*Exercises*, *Homework assignment, Workshops*) – **55 %** of the final grade
  - Solutions should be submitted using course Website
    - Use - ***Upload function***
  - Solution file should be in ***PDF*** format.
  - There must be ***authors name and surname*** indicated in the submission file (written on the solution sheet).

  Grade '0' will be given if any of these requirements is not fulfilled.

  - Deadline to submit solutions - **23:59**, **Tuesday**
    - of next week after lecture/practicals
    - In case of the late submission - a **penalty of half evaluation points** will be applied.

To be admitted to the exam, at least 30% of grade from the practical assignments needs to be collected during the semester

- **Exam** – **45 %** of the final grade

Modalities and Assessment

- **Practicals** (*Exercises*, *Homework assignment, Workshops*) – **55 %** of the final grade
  - Solutions should be submitted using course Website
    - Use - ***Upload function***
  - Solution file should be in ***PDF*** format.
  - There must be ***authors name and surname*** indicated in the submission file (

  Grade **fulfilled**.

  - Dea
    assi
    -
    - be applied.

To be ad **practical**
as **ster**

Exam dates

1.June – first time

OR

8.June – second time

15.June – *resit exam*

- **Exam** – **45 %** of the final grade

Previous Year Feedback

- Focus on the assignments and practice session.
- Having workshops after every class (almost every) cemented the implementation of models and reinforced the notes presented in the lecture.

- It is an awesome course, if you pay attention and work every week.
- The amount of independent work was quite a lot. It took about 6 hours per week to do properly. But it had to be done to learn about the topic.

- This course killed my all two days in week during the semester.
- This course will destroy your most of your free time in second semester and at the end don't expect to get good grade. Just be happy that you will pass this course.

Lecture 1: Introduction

Security Risk Management

- **Dubois E., Heymans P., Mayer N., Matulevičius R.,** A Systematic Approach to Define the Domain of Information System Security Risk Management, Nurcan, S.; Salinesi C.; Souveyet C.; Ralyte, J. (eds.) *Intentional Perspectives on Information Systems Engineering*, 2010, pp. 289-306

Motivation

- ❖ Computer systems and software play an important role in different areas of human life
- ❖ Confidential information

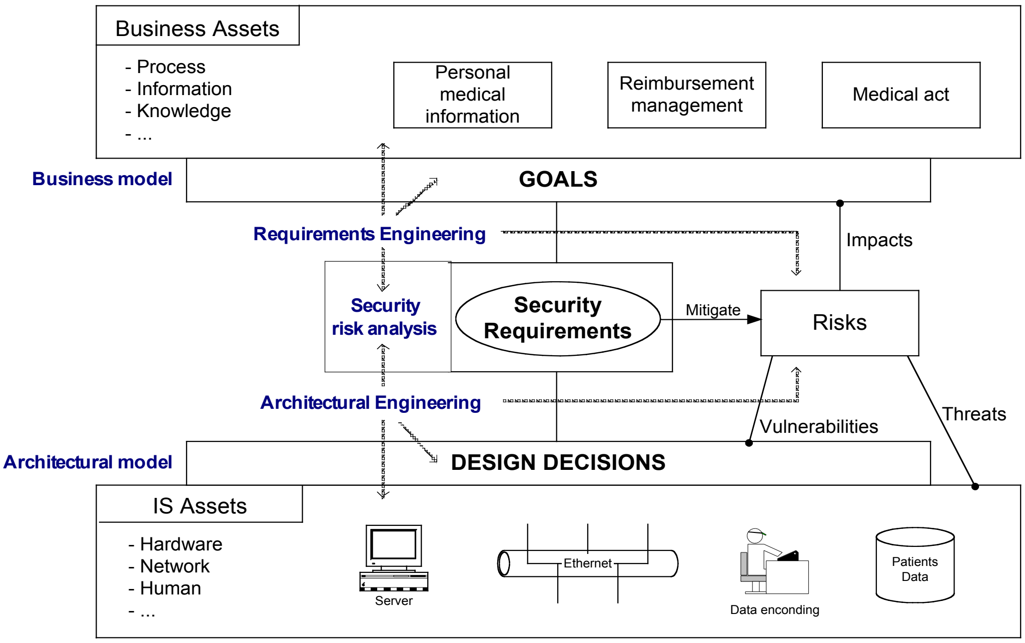
Bank account

Educational qualification

Health records

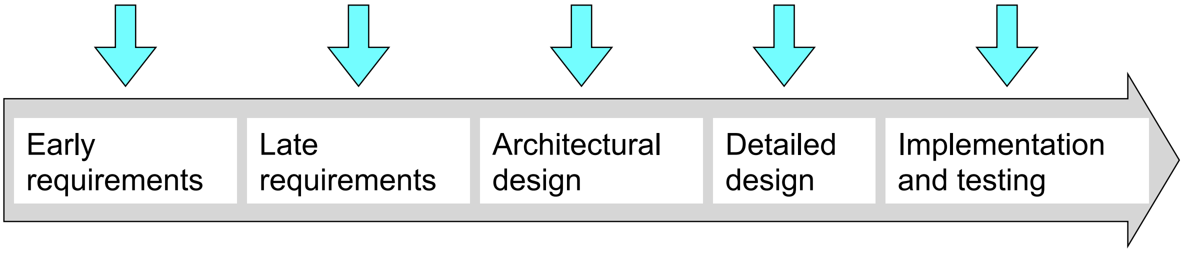
- ❖ The need to secure systems and software becomes a necessity rather than an option

Security Risks in Information Systems



Security from early phases

Security analysis should be performed through the whole software development process



Early requirements

Late requirements

Architectural design

Detailed design

Implementation and testing

- ❖ Early consideration of security allows modellers to
  - envisage threats, their consequences and countermeasures
  - discard design alternatives that do not offer a sufficient security level
  - re-scope or cancel a project if the risk is too high

What is **System**?

- Component
  - – smartcard, a PC or piece of software
- Infrastructure
  - – Operating system, network, etc
- Applications
- IT staff
- Internal users and management
- Customers and external users
- **Environment**

Anderson, 2008

What is **System**?

- Component
  - – smartcard, a PC or piece of software
- Infras
  - – Op
- Applic
- IT sta
- Internal users and management
- Customers and external users
- Environment

EVERYTHING !!!

How to Crack Encrypted Message?

- Acquire massive amount of computing power and brute-force **all** the possible values of the encryption key?
  - The cryptographer's dream scenario

A CRYPTO NERD'S IMAGINATION:
HIS LAPTOP'S ENCRYPTED. LET'S BUILD A MILLION-DOLLAR CLUSTER TO CRACK IT.
NO GOOD! IT'S 4096-BIT RSA!
BLAST! OUR EVIL PLAN IS FOILED!

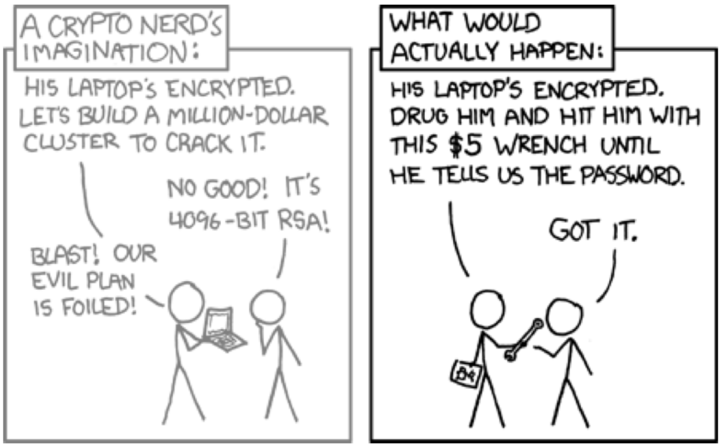
How to Crack Encrypted Message?

- Although, what about the case where the key is **easily guessable password**?

password
123456
12345678
qwerty
abc123
monkey
1234567
letmein
trustno1
dragon
baseball
111111
Iloveyou
master
sunshine
ashley
bailey
passw0rd
shadow
123123
654321
superman
qazwsx
michael
football

How to Crack Encrypted Message?

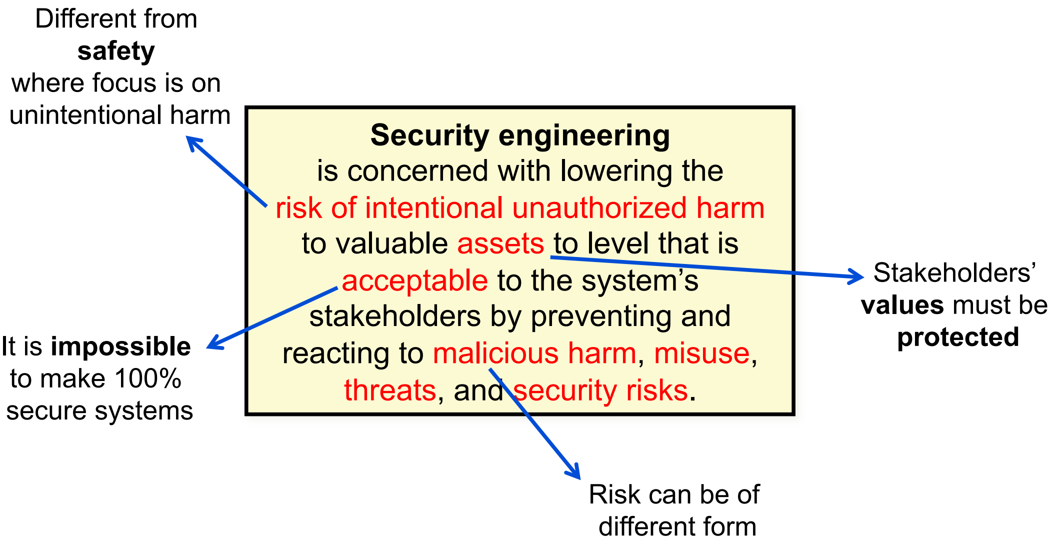
- Or, better yet, why not **just ask** for password?


A CRYPTO NERD'S IMAGINATION:
HIS LAPTOP'S ENCRYPTED. LET'S BUILD A MILLION-DOLLAR CLUSTER TO CRACK IT.
NO GOOD! IT'S 4096-BIT RSA!
BLAST! OUR EVIL PLAN IS FOILED!
WHAT WOULD ACTUALLY HAPPEN:
HIS LAPTOP'S ENCRYPTED. DRUG HIM AND HIT HIM WITH THIS $5 WRENCH UNTIL HE TELLS US THE PASSWORD.
GOT IT.

How to Crack Encrypted Message?

- How about accessing the computer and **installing key-logger** or **trojanised** version of the message viewer?
  - Maybe there is already has some **remote-controlled malware** installed
  - Maybe the decrypted message could be **read from computer's memory** or **hard disk**?

What is **Security engineering**?



Different from **safety** where focus is on unintentional harm

Security engineering is concerned with lowering the risk of intentional unauthorized harm to valuable assets to level that is acceptable to the system's stakeholders by preventing and reacting to malicious harm, misuse, threats, and security risks.

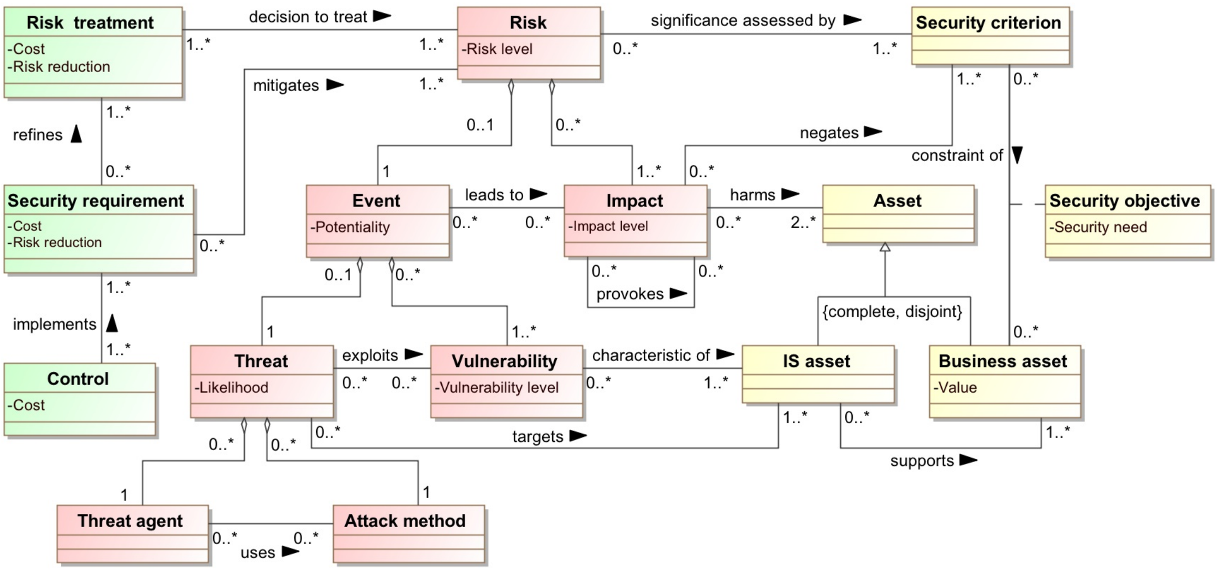
Stakeholders' **values** must be **protected**

It is **impossible** to make 100% secure systems

Risk can be of different form

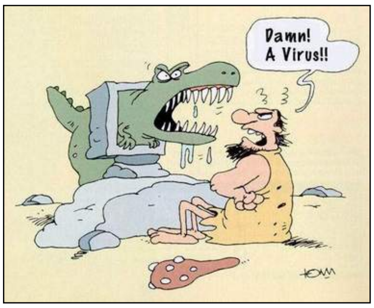
Firesmith, 2003

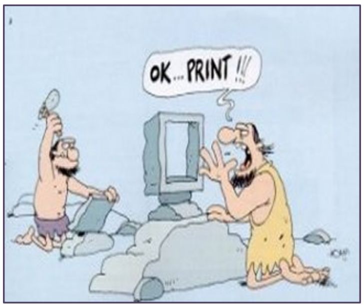
Security Risk Management Domain Model



Mayer, Dubois *et al.*, 2008

Major Terminology





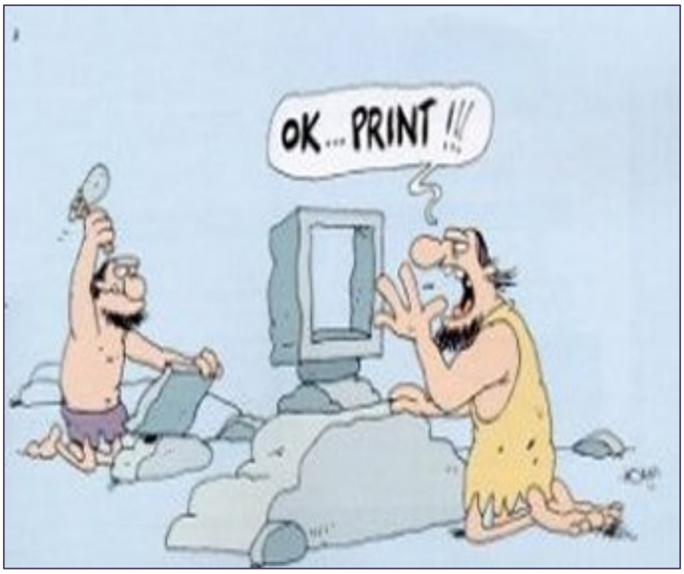
- Risk treatment decisions
- Security requirements
- Controls

- Risk
- Impact
- Event
- Vulnerability
- Threat
- Threat agent
- Attack method

- Assets
  - Business assets
  - IS assets
- Security criterion

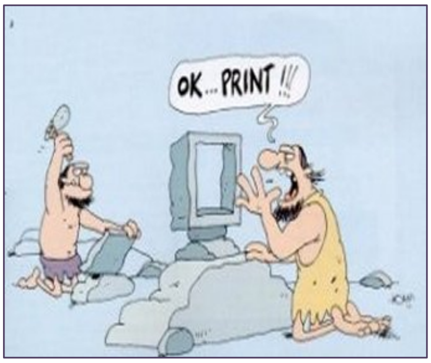
Asset-related concepts

- Important assets to protect, and what are the criteria to guarantee asset security



Asset

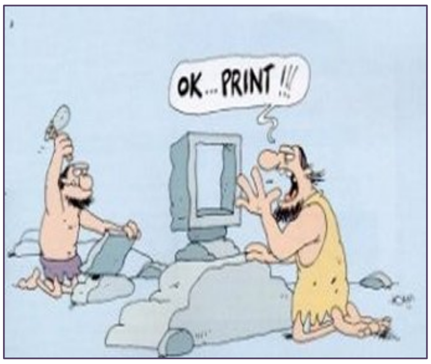
- **Asset**
  - anything that has value to the organisation and is necessary for achieving its objectives
    - *technical plan*
    - *structure calculation process*
    - *architectural competence*
    - *operating system*
    - *Ethernet network*
    - *people encoding data*
    - *system administrator*
    - *air conditioning of server room*



- This concept is the generalisation of the **business asset** and **IS asset** concepts

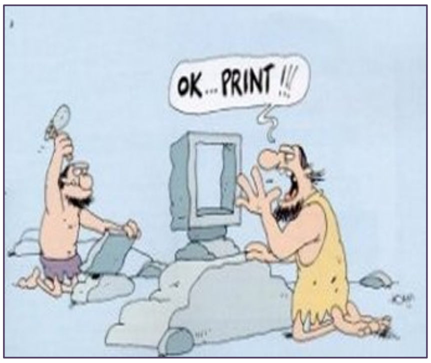
Business asset

- **Business asset**
  - information, process, skill inherent to the business of the organisation that has value to the organisation in terms of its business model and is necessary for achieving its objectives
    - *technical plan*
    - *structure calculation process*
    - *architectural competence*
- **Business assets are immaterial**



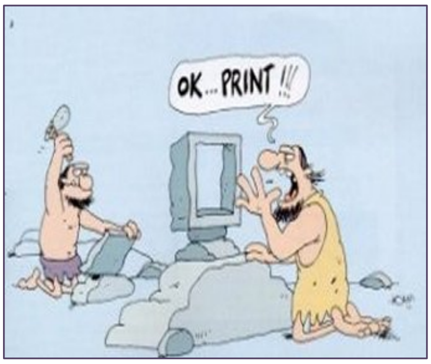
IS asset

- **IS asset**
  - a component or part of the IS that has value to the organisation and is necessary for achieving its objectives and supporting business assets
    - *operating system*
    - *Ethernet network*
    - *people encoding data*
    - *system administrator*
    - *air conditioning of server room*
- **IS assets are material**
  - with the exception of software



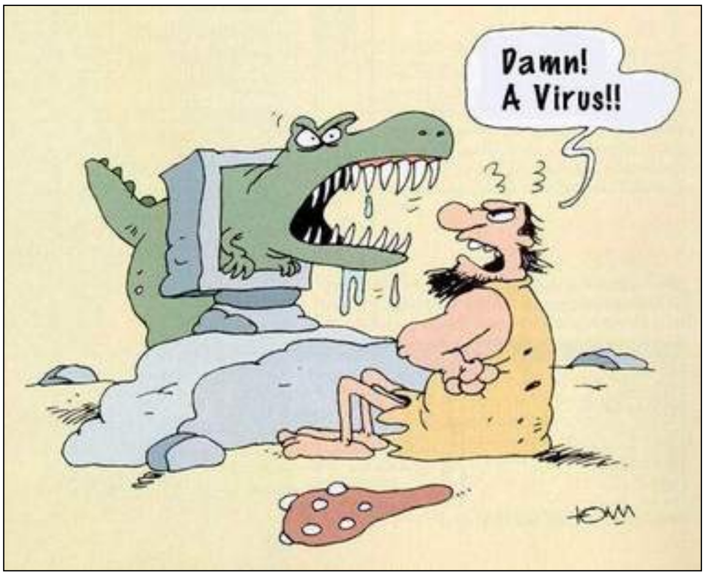
Security criterion

- **Security criterion**
  - property or constraint on business assets that characterises their security needs
  - act as indicators to assess the significance of a risk
    - *Confidentiality*
    - *Integrity*
    - *Availability*
- **The security objectives of an IS are defined using security criteria on business assets**
    - *Confidentiality of the technical plans*
    - *Integrity of the structure calculation process*



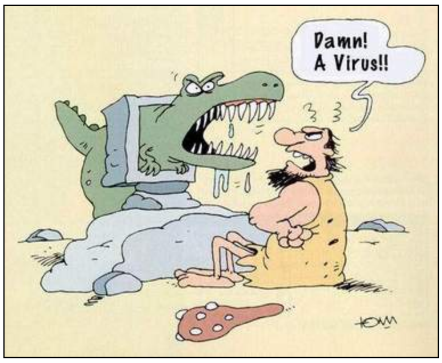
Risk-related concepts

- How the risk itself and its immediate components are defined



Risk

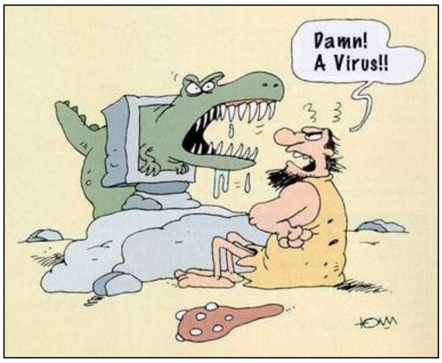
- **Risk**
  - combination of a **threat** with one or more **vulnerabilities** leading to a negative **impact** harming at least two or more of the **assets**
    - *A hacker using social engineering on a member of the company, because of weak awareness of the staff, leading to unauthorised access to personal computers and loss of integrity of the structure calculation process*



- **Threat** and **vulnerabilities** are part of the risk **event** and **impact** is the consequence of the risk.

Impact

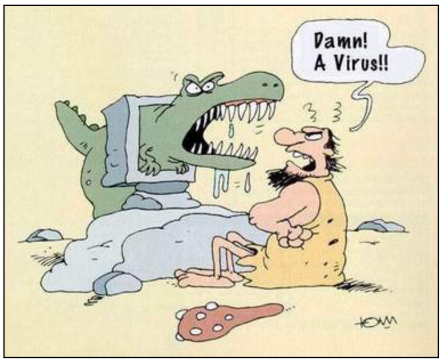
- **Impact**
  - potential negative consequence of a risk that may harm assets of a system or an organisation, when a threat is accomplished
    - *password discovery* (**impact on IS assets**)
    - *data destruction*
    - *failure of a component*
    - *a loss of confidentiality of technical plans* (**impact on business assets**)
    - *a loss of confidentiality of an information*
    - *a loss of integrity of a process*



- **An impact can provoke a chain reaction of impacts (or indirect impacts)**
    - *a loss of confidentiality on sensitive information leads to a loss of customer confidence*

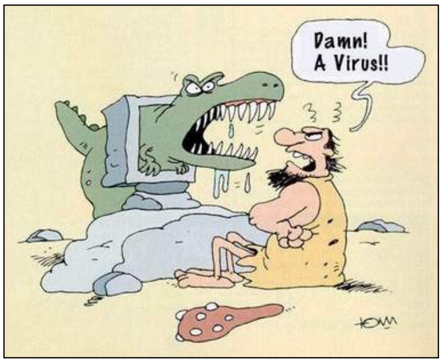
Event

- **Event**
  - combination of a threat and one or more vulnerabilities
    - *a hacker using social engineering on a member of the company, exploiting weak awareness of the staff*
    - *a thief entering a company building thanks to deficient physical access control*



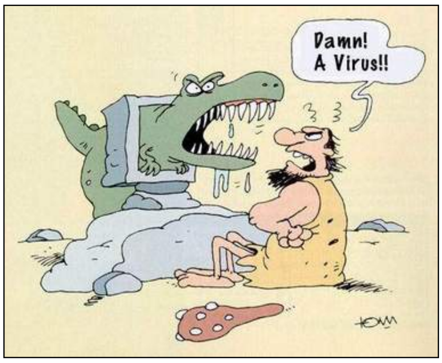
Vulnerability

- **Vulnerability**
  - characteristic of an IS asset or group of IS assets that can constitute a weakness or a flaw in terms of IS security
    - *weak awareness of the staff*
    - *deficient physical access control*
    - *lack of fire detection*



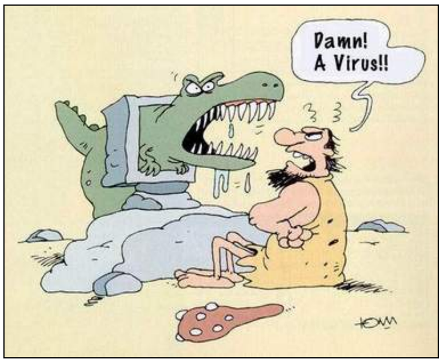
Threat

- **Threat**
  - potential attack, carried out by an agent that targets one or more IS assets and that may lead to harm to assets
    - *a hacker using social engineering on a member of the company*
    - *a thief entering a company building and stealing media or documents*



Threat agent

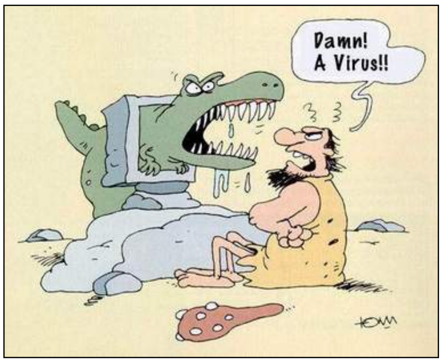
- **Threat agent**
  - an agent that can potentially cause harm to assets of the IS
  - triggers a threat and is the source of a risk
    - *staff members with little technical skills and time and possibly a strong motivation to carry out an attack;*
    - *hacker with considerable technical skills, well equipped and strongly motivated by the money he could make*



- **A threat agent can be characterised by expertise, available resources and motivation**

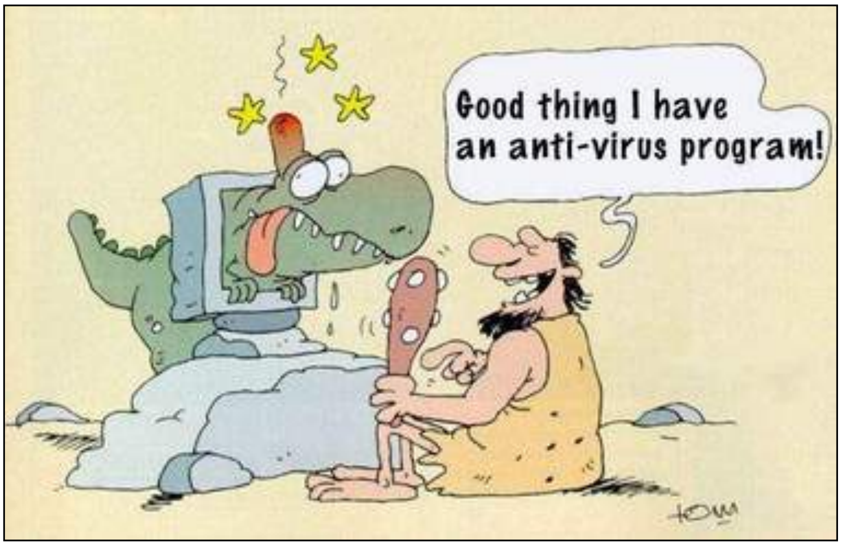
Attack method

- **Attack method**
  - standard means by which a threat agent carries out a threat
    - *system intrusion*
    - *theft of media or documents*



Risk treatment-related concepts

- What decisions, requirements and controls should be defined and implemented in order to mitigate possible risks



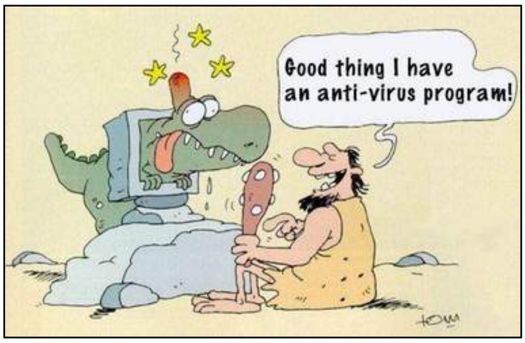
Risk treatment

- **Risk treatment**
  - decision of how to treat the identified risks
  - satisfies a security need, expressed in generic and functional terms, and can lead to security requirements
    - **Risk avoidance**
    - **Risk reduction**
    - **Risk transfer**
    - **Risk retention**

Risk treatment

Risk avoidance

- **Risk avoidance**
  - Decision not to become involved in, or to withdraw from, a risk
  - Functionality of the IS are modified or discarded for avoiding the risk
    - *not connecting the IS to the Internet*



Risk treatment

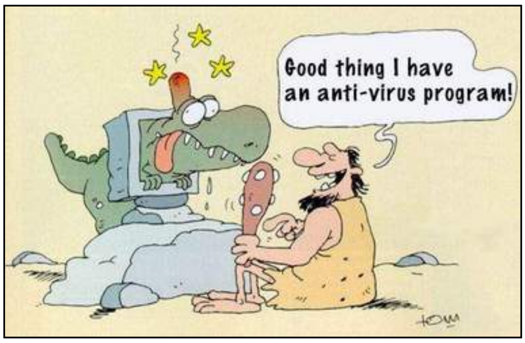
Risk reduction

- **Risk reduction**
  - Action to lessen the probability, negative consequences, or both, associated with a risk
  - Security requirements are selected for reducing the risk
    - *taking measures to avoid network intrusions*

Risk treatment

Risk transfer

- **Risk transfer**
  - Sharing with another party the burden of loss from a risk.
  - A third party is thus related to the (or part of the) IS, ensuing sometimes some additional security requirements about third parties
    - *taking an insurance for covering a loss of service*



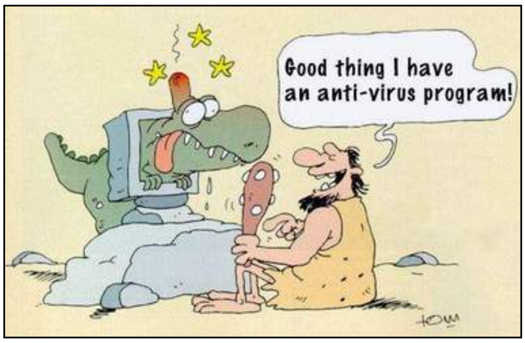
Risk treatment

Risk retention

- **Risk retention**
  - Accepting the burden of loss from a risk
  - No design decision is necessary in this case
    - *accepting that the service could be unavailable for 1 hour*

Security requirement

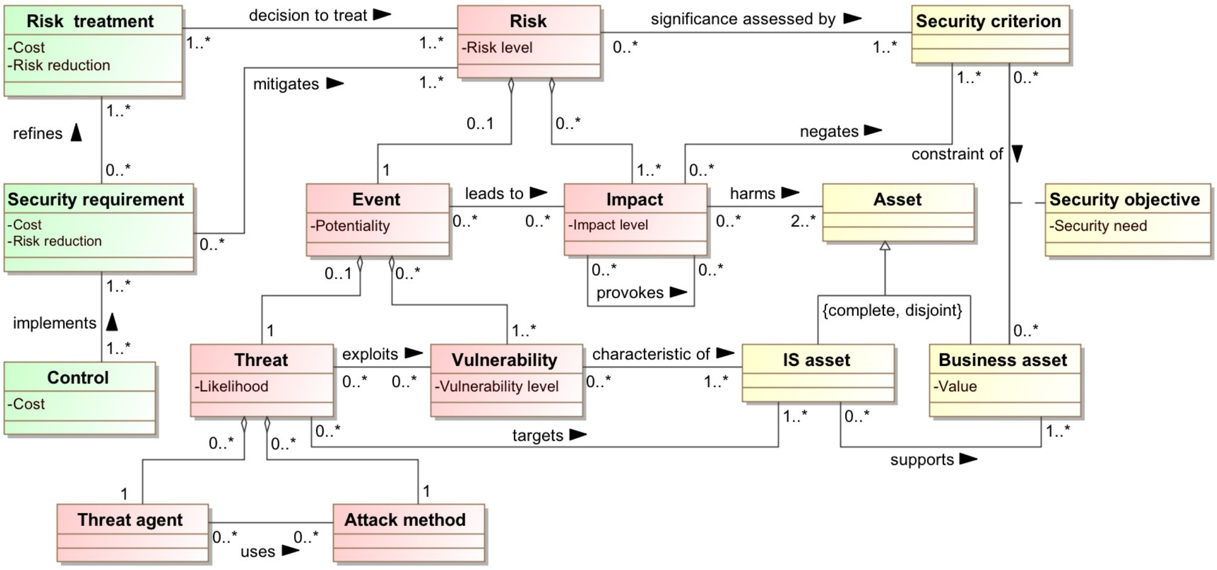
- **Security requirement**
  - a condition over the phenomena of the environment that we wish to make true by installing the IS, in order to mitigate risks
    - *appropriate authentication methods shall be used to control access by remote users*
    - *system documentation shall be protected against unauthorised access*



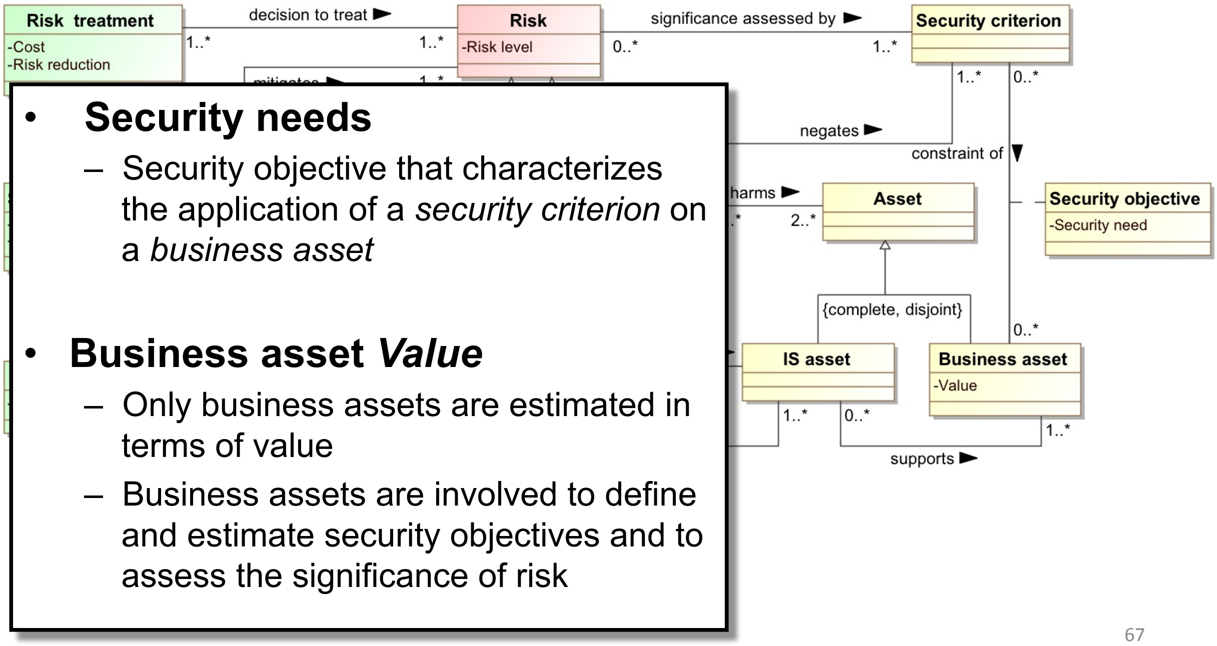
Control

- **Control**
  - designed means to improve security, specified by a security requirement, and implemented to comply with it
    - Examples: *firewall; backup procedure; building guard.*

Security Risk Management Domain Model

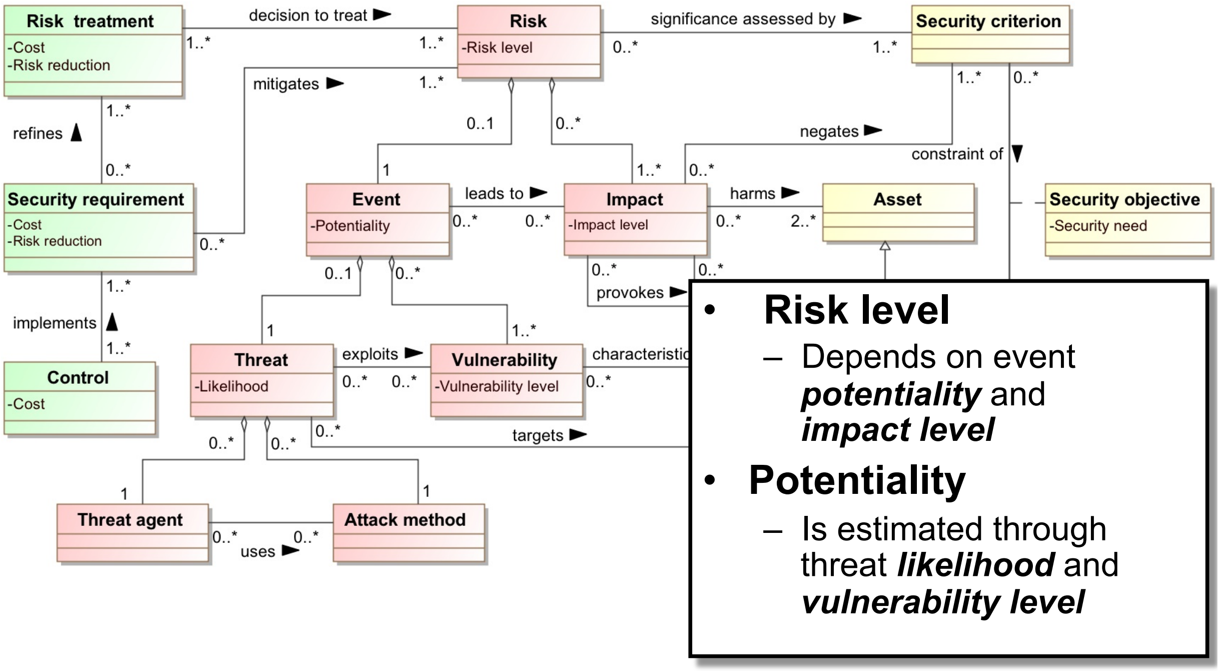


Security Risk Management Domain Model



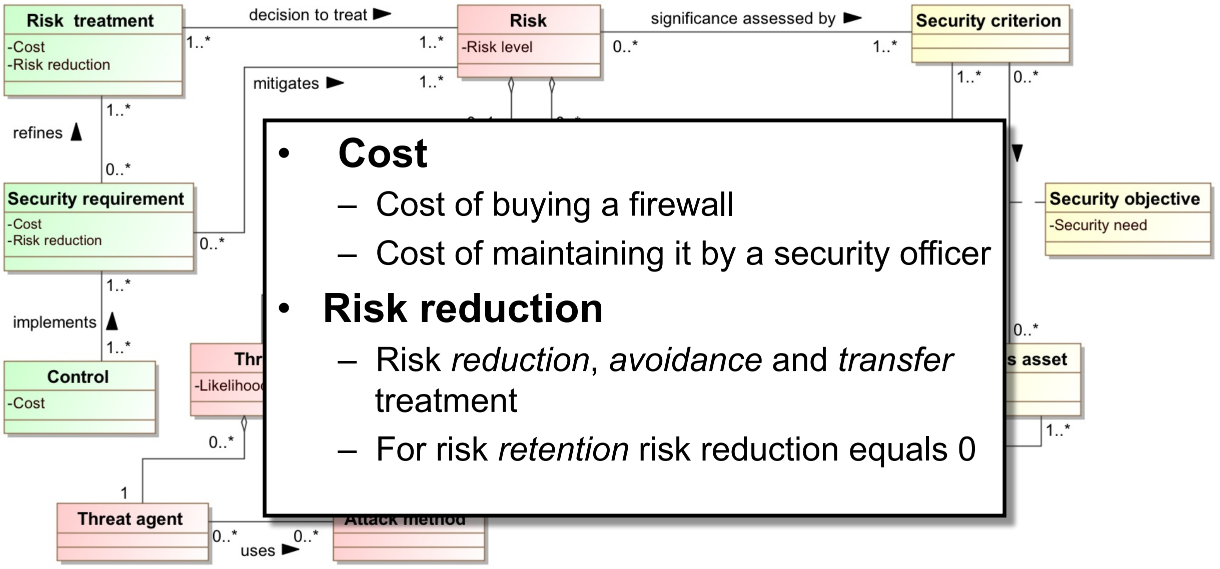
- **Security needs**
  - Security objective that characterizes the application of a *security criterion* on a *business asset*
- **Business asset *Value***
  - Only business assets are estimated in terms of value
  - Business assets are involved to define and estimate security objectives and to assess the significance of risk

Security Risk Management Domain Model



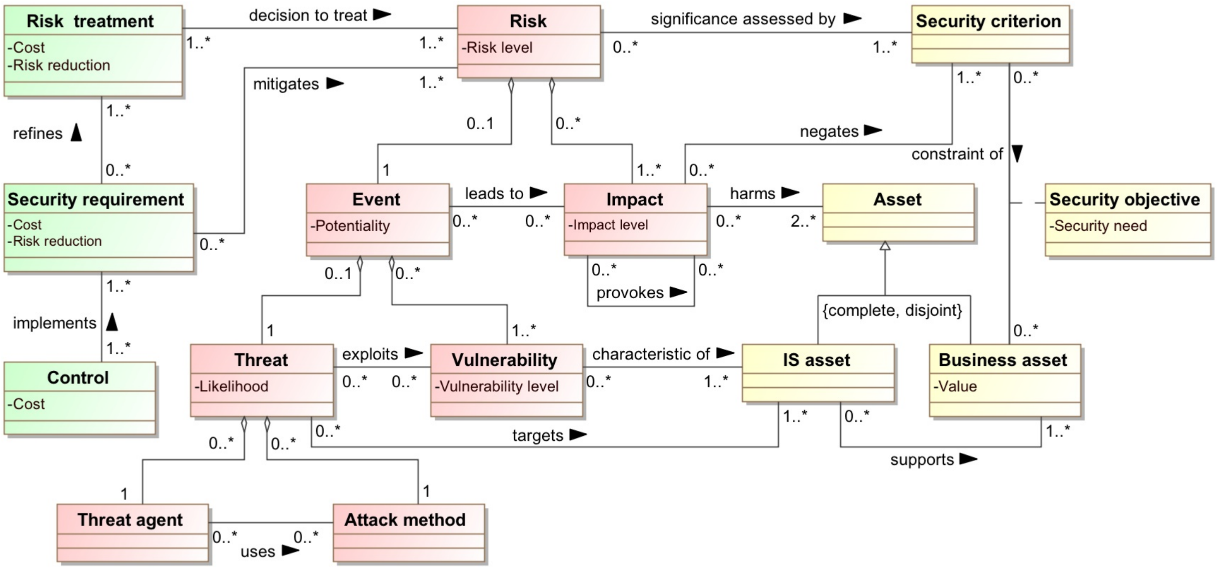
- **Risk level**
  - Depends on event ***potentiality*** and ***impact level***
- **Potentiality**
  - Is estimated through threat ***likelihood*** and ***vulnerability level***

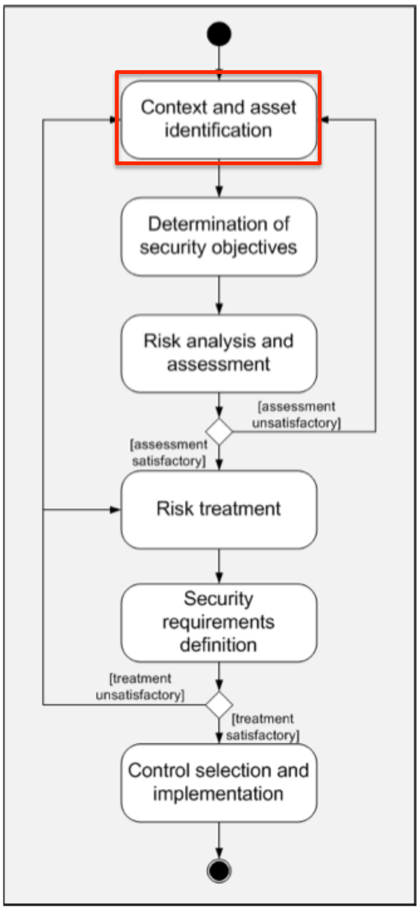
Security Risk Management Domain Model



- **Cost**
  - Cost of buying a firewall
  - Cost of maintaining it by a security officer
- **Risk reduction**
  - Risk *reduction*, *avoidance* and *transfer* treatment
  - For risk *retention* risk reduction equals 0

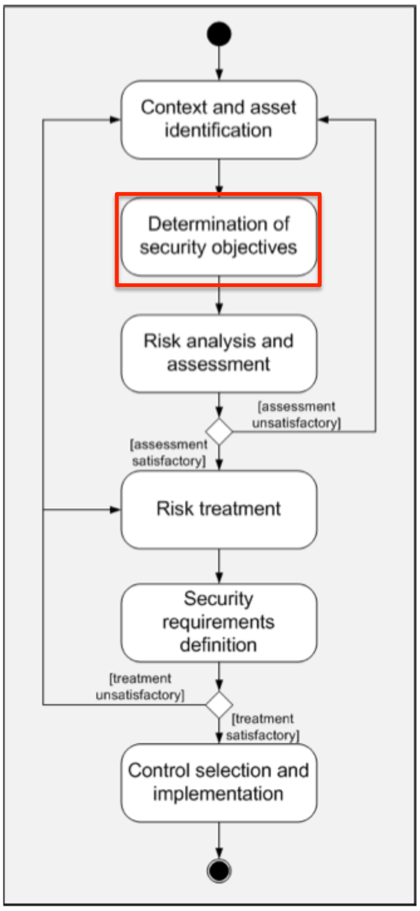
Security Risk Management Domain Model




Context and asset identification
Determination of security objectives
Risk analysis and assessment
[assessment unsatisfactory]
[assessment satisfactory]
Risk treatment
Security requirements definition
[treatment unsatisfactory]
[treatment satisfactory]
Control selection and implementation

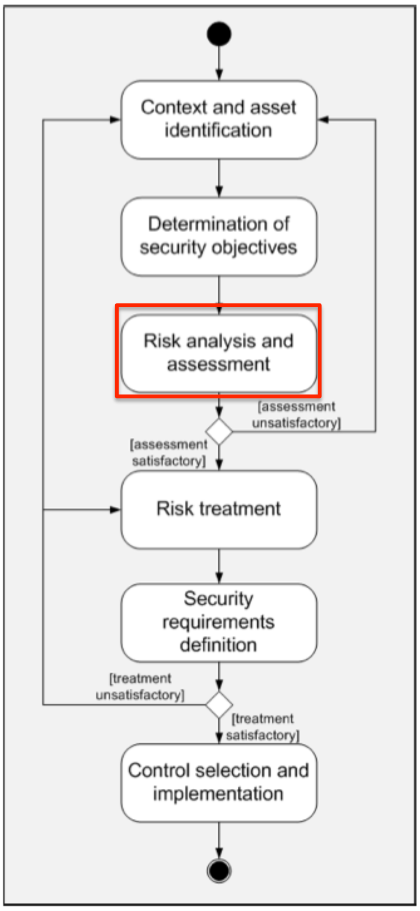
Security risk management process

- Description of organisation and its environment
  - sensitive activities related to information security
  - Example:
    - *Design of technical plans*
    - *The technical plans are created by drawers and engineers on computers connected to the Internet*


Context and asset identification
Determination of security objectives
Risk analysis and assessment
[assessment unsatisfactory]
[assessment satisfactory]
Risk treatment
Security requirements definition
[treatment unsatisfactory]
[treatment satisfactory]
Control selection and implementation

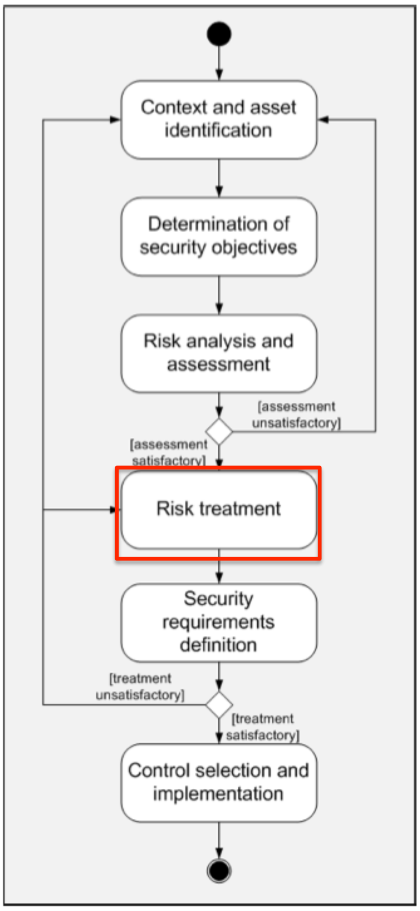
Security risk management process

- Determine the security objectives to be reached
  - Confidentiality, Integrity, Availability
  - Example:
    - *During their design, the technical plans should be kept confidential*


Context and asset identification
Determination of security objectives
Risk analysis and assessment
[assessment unsatisfactory]
[assessment satisfactory]
Risk treatment
Security requirements definition
[treatment unsatisfactory]
[treatment satisfactory]
Control selection and implementation

Security risk management process

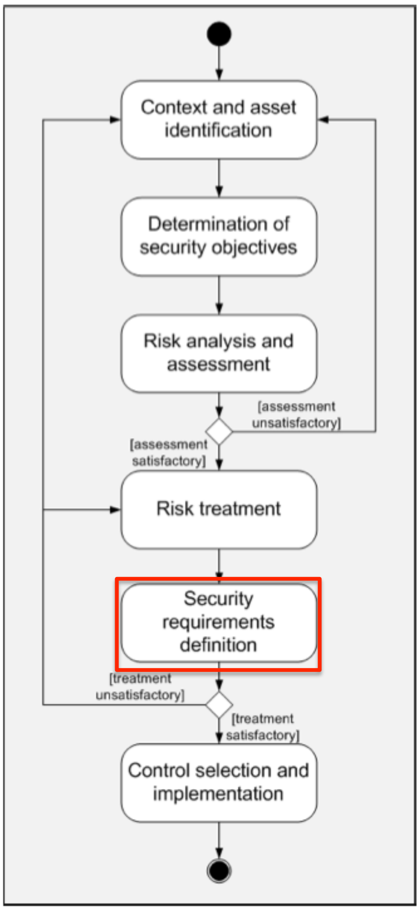
- Identify risks and estimate them qualitatively or quantitatively
  - Example:
    - *A rival of tries to use common operating system and network protocol weaknesses to penetrate on the personal computer of an employee, where confidential technical plans are stored.*
    - *Estimated level: sufficiently high*


Context and asset identification
Determination of security objectives
Risk analysis and assessment
[assessment unsatisfactory]
[assessment satisfactory]
Risk treatment
Security requirements definition
[treatment unsatisfactory]
[treatment satisfactory]
Control selection and implementation

Security risk management process

- Risk treatment measures
  - Risk avoidance
  - Risk reduction
  - Risk transfer
  - Risk retention

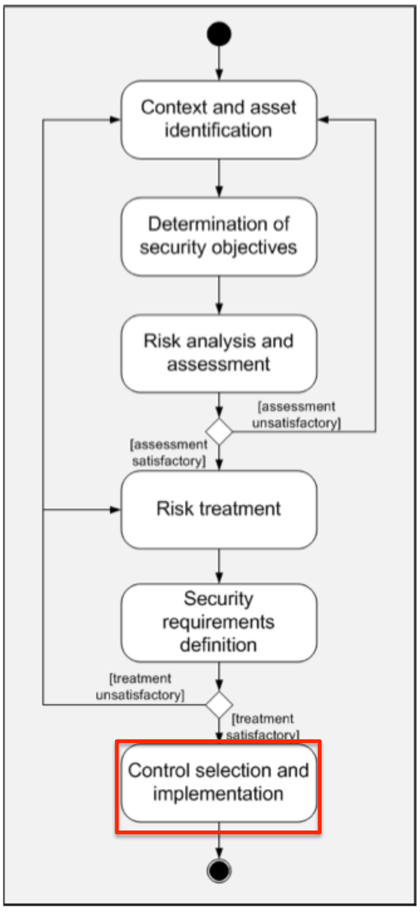
  - Example:
    - Reduce the preceding risk with some security controls implemented in the IS


Context and asset identification
Determination of security objectives
Risk analysis and assessment
[assessment unsatisfactory]
[assessment satisfactory]
Risk treatment
Security requirements definition
[treatment unsatisfactory]
[treatment satisfactory]
Control selection and implementation

Security risk management process

- Security requirements - security solutions to mitigate the risks
- If security requirements are unsatisfactory
  - Revise the risk treatment step
  - Revise all of the preceding steps

  - Example:
    - Procedures for monitoring the use of information processing facilities should be established and the results of the monitoring activities reviewed regularly



Context and asset identification

Determination of security objectives

Risk analysis and assessment

[assessment unsatisfactory]

[assessment satisfactory]

Risk treatment

Security requirements definition

[treatment unsatisfactory]

[treatment satisfactory]

Control selection and implementation

Security risk management process

- Implement system countermeasures within organisation
  - Example:
    - A firewall and an Intrusion Detection System (IDS) are selected and implemented

What have we learnt?

- Security Engineering
- Domain model for Security Risk Management
  - Assets
  - Risks
  - Risk treatment
- Security Risk Measurement
- Security Risk Management Process