System development

# IT security

|  |  |
| --- | --- |
| Exercise name | Ex50Wed-IT-security |
| Learning goals | After doing this exercise you should   * have knowledge of how IT security can fail * be able to make a risk assessment * be able to make a plan for how to minimize risks. |
| Expected outcome | When you have done this exercise your team should have produced   * A list of it systems you use * A list of incidents that can threaten your IT security * prioritized lists of elements you want to quality assure and for each |

Prepare for the exercises by

* Read the chapter “IT security” in “On track of the good system”.
* Consider your own use of it
  + what risks can you have?
  + How serious are the risks for you?

In these exercises you will assess your own IT security and risk, and make a plan for improvement.

The exercises will be solved in teams of 4, but every team member makes their own answers.

# Exercise 1 How can IT security fail?

IT security can fail in 3 ways:

* Data is inaccessible
* Errors occur in systems or data
* Sensitive data is not protected

And an incident can be

* Internal intentional
* External intentional
* Internal accidental
* External accidental
* Technical accidental

## Exercise 1.01, the system

To assess the risk, we must first make ​​an overview of the entire IT system. This includes both the systems in use in project assignments, homework, communication, social purpose, practical private purposes etc.

Using **placemat consensus**, you should make a list of systems.

At first, you make a list of all the systems, you think you have, on your own.

Use **Round Robin** to make a longer list: the first group member says a system from his/her list, another group says a system from his/her list which is not already mentioned, the third group member .... Until all systems are put on a long list that you can work with

*Timeframe: 5 minutes + 10 minutes*

## Exercise 1.02, incidents

The next thing we need to do is to consider which incidents that may threaten our IT security. The way to do this is to consider the ways in which safety can fail in each system and what type of incident it will be.

Use **Round Robin** to find as many as possible: The first group member takes an event and explains how the security on this count and what type it is, the second group member takes a different event and explains how the security on this count and what type it is, etc.

Make sure both to cover all systems, all ways and all types!

*Timeframe: 20 minutes*

# Exercise 2, Assessment of risk

For each of the relevant incidents assess three factors:

• Economic impact : what does it cost you (the company) if the incident has occured?  
• Your (The company's) vulnerability : how well you (the company) is protected from the incident ?  
• Threat : how likely is it that you (the company) are exposed to the incident ?

## Exercise 2.01, impact

Make a form:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Education | Job | Social | ….. |
| Incident 1 |  |  |  |  |
| Incident 2 |  |  |  |  |
| Incident 3 |  |  |  |  |
| … |  |  |  |  |
| … |  |  |  |  |

If it had been for a company you would only be looking at the economic impact, but because you are not a company, here we are just looking at the overall impact - how bad would it be if this incident occurred? Rate for different parts of your life.

Use the values ​from the scale:

* + low (it does not matter)
  + between (it will be quite annoying)
  + high (it will be disastrous)

Use **Round Robin** to complete the form, discuss why you put a certain value on an impact, but remember that you do not have to agree.

*Timeframe: 20 minutes*

## Exercise 2.02 vulnerability

Here we have to assess how vulnerable we are to the individual incident - that is, have we already done something to counter the incident?

For the assessment of vulnerability use again the scale:

* + Low
  + Medium
  + high

Use **think-pair-share**

First make a form each that you fill with the value you think each incident has.

|  |  |
| --- | --- |
|  | **Vulnerability** |
| Incident 1 |  |
| Incident 2 |  |
| Incident 3 |  |
| … |  |

Then discuss you answers as a pair – remember you don’t have to reach agreement

Finally discuss your answers in the team.

*Timeframe: 5 + 10 + 5 minutes*

## Exercise 2.03 Threat

Here we to have assess how big a threat is the individual incident? How likely is it that the incident will occur?

For the assessment of threat use the scale:

* + Low
  + Medium
  + high

Use **think-pair-share**

First make a form each, that you fill with the value you think each incident has.

|  |  |
| --- | --- |
|  | **Threat** |
| Incident 1 |  |
| Incident 2 |  |
| Incident 3 |  |
| … |  |

Then discuss your answers as a pair – remember you don’t have to reach agreement

Finally discuss your answers in the team.

*Timeframe: 5 + 10 + 5 minutes*

## Exercise 26.04 Total risk

We have now put values ​​on impact, vulnerability and threat for each incident. The next step is to calculate the total risk for each incident. Use the method from the note to do the calculation.

*Timeframe: 15 minutes*

# Exercise 3, Make a plan

## When faced with a risk, there are two ways you can handle it. You can make a plan for how to prevent the incident and / or you can make a plan on how to compensate for the damage the incident causes.

## Exercise 3.01 the Plan

You must now make a plan for the incidents that have a risk of high and medium. Use **Round Robin** to find out what your plan of action should be for each incident, and fill out the form:

|  |  |  |  |
| --- | --- | --- | --- |
|  | Risc assessment | existing hedge | Action plan |
| Incident 1 |  |  |  |
| Incident 2 |  |  |  |
| Incident 3 |  |  |  |
| … |  |  |  |

*Timeframe: 40 minutes*