Oblig III on security risk assessment

INF5150

by Magnus W. Østeng

Oblig III on security risk assessment

INF5150

A.

How many risk values are defined by the matrix?

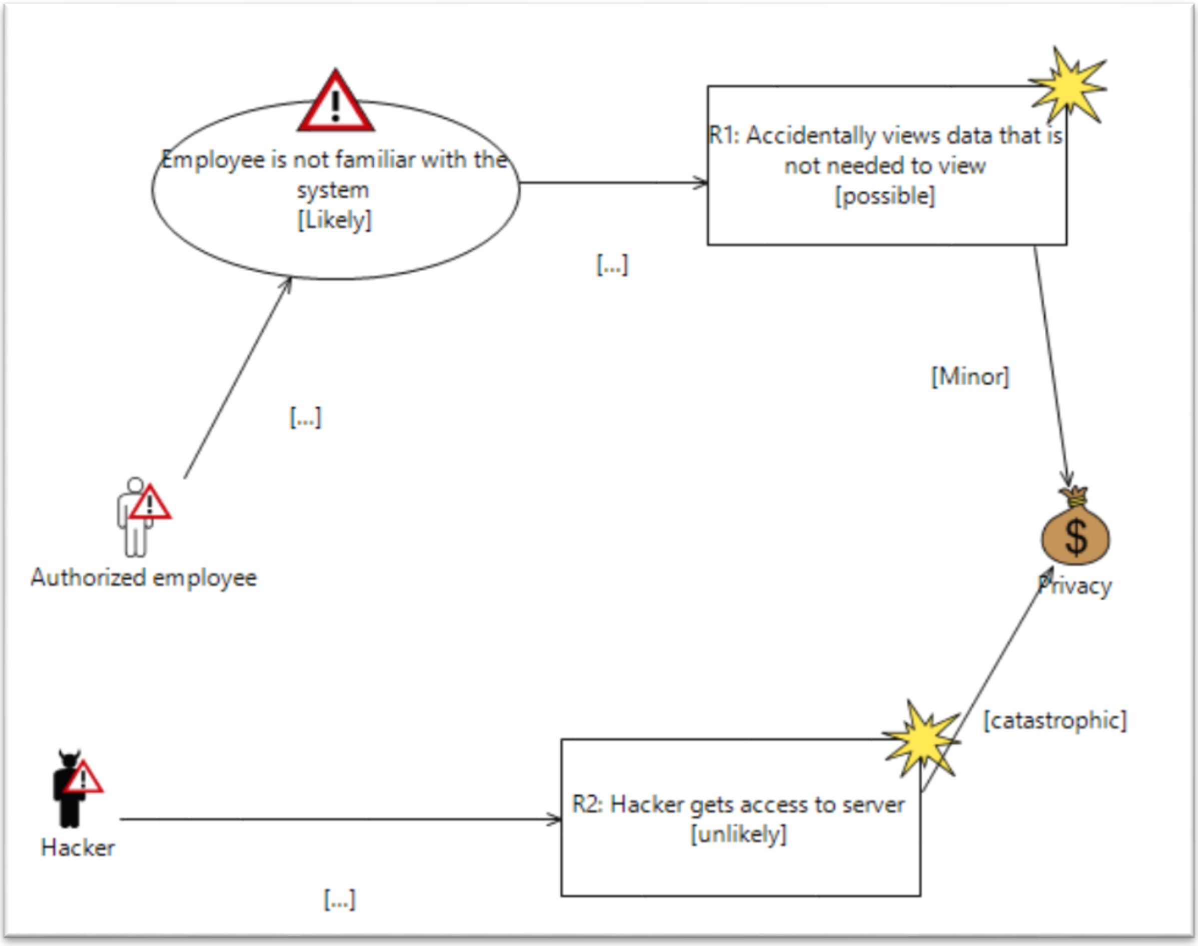
In this example there are three different risk value:

- Green: corresponds with for example risk value “low”
- Yellow: corresponds with for example risk value “medium”
- Red: corresponds with for example risk value “high”

The risk values are defined on the terms of the consequence scale and the likelihood scale in the matrix. There is no right way to define the risk value, because they are different in each scenario. For instance, in a banking system, Risk value 1 (R1) could be define as risk value medium (Yellow) if the risk must be considered for possible treatment. So it entirely depends on what kind of system we operate with and what we can accept of risks.

B.

Assume R1 and R2 are risks with respect to the asset privacy. Draw a syntactically correct and consistent CORAS threat diagram representing both R1 and R2 as defined by the risk matrix in Figure 1. Argue why it is consistent.


Employee is not familiar with the system
[Likely]
R1: Accidentally views data that is not needed to view
[possible]
[...]
[Minor]
[...]
Authorized employee
Privacy
[catastrophic]
Hacker
R2: Hacker gets access to server
[unlikely]
[...]

In this threat diagram R1 is represented by the unwanted incident generated by the Employee and R2 as the unwanted incident generated by the Hacker.

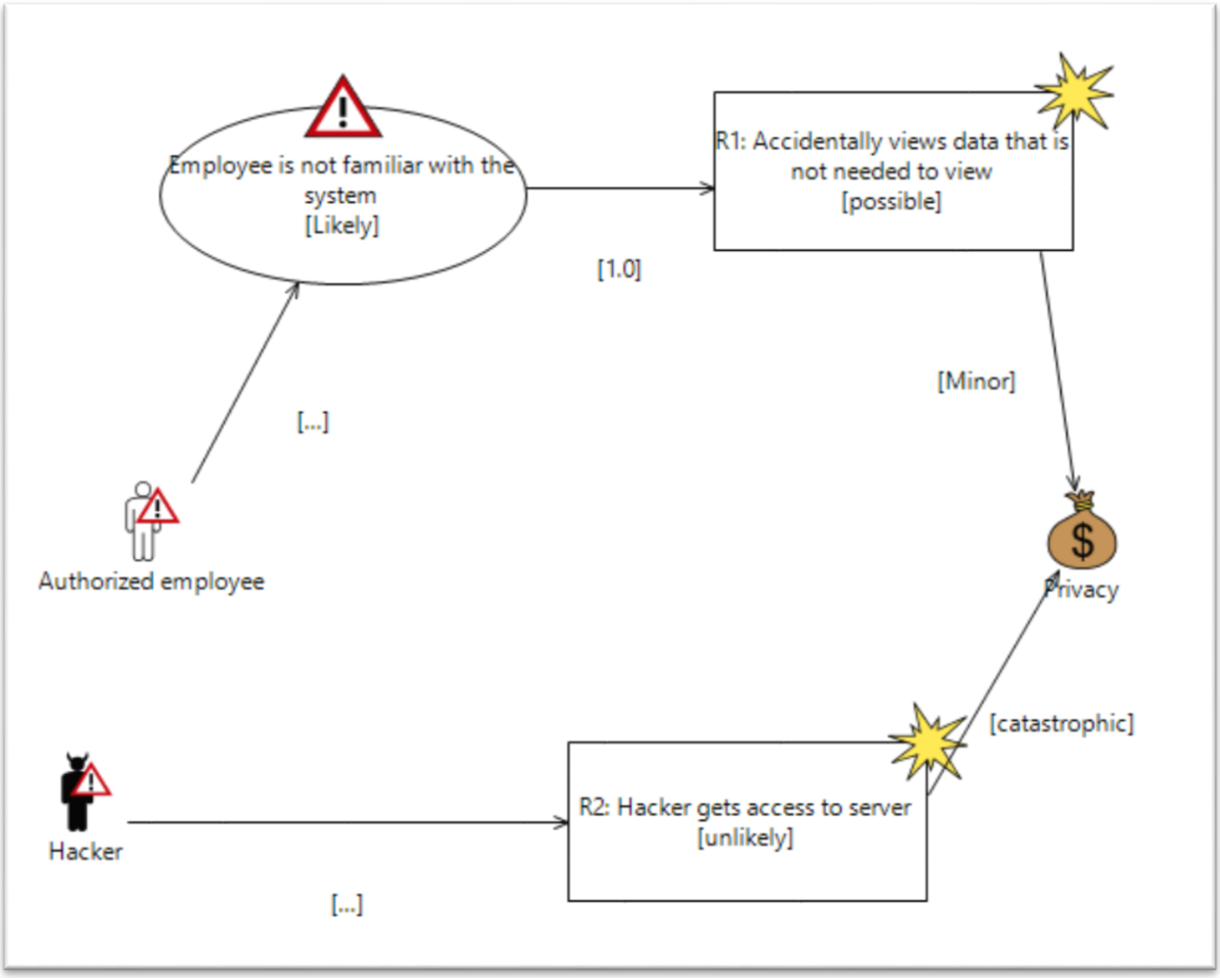
Privacy is the asset and considered to be privacy of personal data, in this case stored in a database system. So if an employee accidentally views a personal data record that he or she does not need to, to do their job, this has a minor impact on the privacy, because the employee is authorized for the system, but not viewing the data on a need-to-know basis.

Threat scenario corresponding to R1 is consistent, because we do not know the conditional (at least I have not made one up). This could mean that the threat scenario corresponding to R1 is considered to have likelihood *possible*. If we consider the threat diagram to be complete, it should be a conditional likelihood, that results in R1 becoming *possible*.

In the R2 part, the diagram is consistent, since there is only one likelihood.

C.

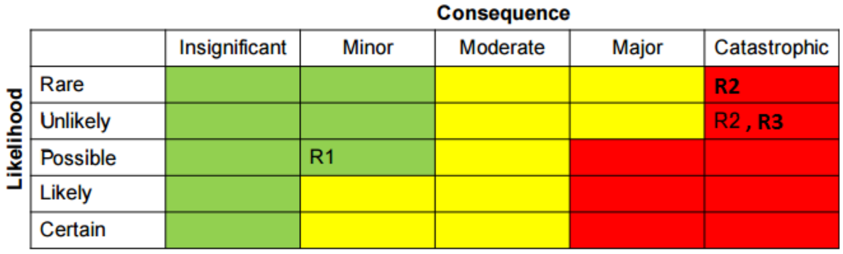
Modify your CORAS threat diagram from b in such a way that it is inconsistent even if it is incomplete? Argue why it is inconsistent.


Employee is not familiar with the system
[Likely]
R1: Accidentally views data that is not needed to view
[possible]
[1.0]
[Minor]
[...]
Authorized employee
Privacy
[catastrophic]
Hacker
R2: Hacker gets access to server
[unlikely]
[...]

This threat diagram becomes inconsistent, because threat scenario "Employee not familiar with the system" with likelihood *likely* has a conditional likelihood *1.0* to cause "Accidentally views data that is not needed to view" [R1] to happen. So this it is fair to assume that every time this threat scenario occurs it certainly leads to R1. This makes no sense because this unwanted incident only occurs with likelihood *possible* which is lower than how often the threat scenario says it should occur. Therefore, we have an inconsistent threat diagram.

D.

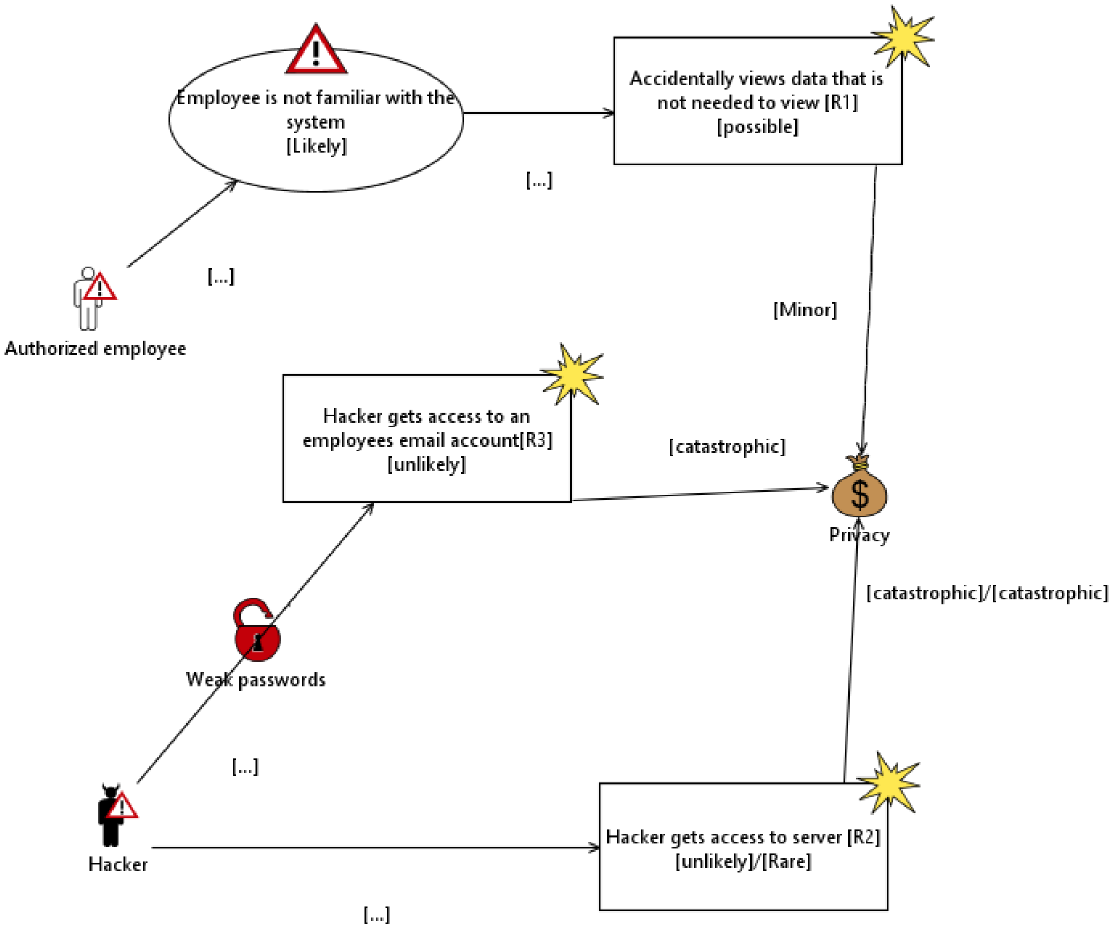
Assume the system for which the risk matrix in Figure 1 is valid, is updated in such a way that the risk R1 disappears, the risk R2 becomes rare (with the consequence unchanged) and we get a new risk to privacy R3 whose consequence is catastrophic. Draw a syntactically correct and consistent CORAS threat diagram in the before-after style matching the new situation in such a way that your old diagram from b is equal to the before part.



		Consequence				
		Insignificant	Minor	Moderate	Major	Catastrophic
Likelihood	Rare	🟩	🟩	🟨	🟨	🟥 **R2**
	Unlikely	🟩	🟩	🟨	🟨	🟥 R2 , **R3**
	Possible	🟩	🟩 R1	🟨	🟥	🟥
	Likely	🟩	🟨	🟨	🟥	🟥
	Certain	🟩	🟨	🟨	🟥	🟥

Figure 1 Risk Matrix

Since there is not specified the likelihood of R3, I give it likelihood unlikely.


Employee is not familiar with the system [Likely]
Accidentally views data that is not needed to view [R1] [possible]
[...]
[...]
Authorized employee
[Minor]
Hacker gets access to an employees email account[R3] [unlikely]
[catastrophic]
Privacy
[catastrophic]/[catastrophic]
Weak passwords
[...]
Hacker
Hacker gets access to server [R2] [unlikely]/[Rare]
[...]

The coras application does not seem to support the shadowing syntax of before-after, so I will instead explain the diagram.

- Because the unwanted incident related to R3 exists only in the after scenario, it should have a black shadow and dotted lines.
- Because the unwanted incident related to R1 exists only in the before scenario it is unchanged.
- Because the unwanted incident related to R2 exists in both scenarios, it should have a white shadow and dotted lines.
- Both the threats and asset exists in both scenarios and should then have white shadows.

E.

Define a qualitative consequence scale for the asset privacy matching Figure 1.

I am defining my qualitative consequence scale as an ordinal scale.

Consequence	Comment
Insignificant	Has none or little effect on privacy. For instance, someone finds out what is your favorite football team.
Minor	It has some degree of effect on privacy. For instance, someone finds your address and phone number.
Moderate	It has a considerable effect on privacy. For instance, someone the postman read all your letters before he puts them in your mailbox.
Major	It has a great effect on privacy. For instance, someone is tapping your phone line. All your phone communication is compromised.
Catastrophic	Privacy is considered compromised. For instance, someone gets hold of your health or economical records and display the information in public.

F.

Define a likelihood scale based on frequencies matching Figure 1.

Redefining the likelihood scale, to a quantitative, ratio scale.

Likelihood	**Interval**
Rare	[0-1:100Y]
Unlikely	<1:100Y-1:5Y]
Possible	<1:5Y-1:1Y]
Likely	<1:1Y-10:1Y]
Certain	<10:1Y, infinite]

It makes more sense to have intervals than fixed frequencies, because fixed frequencies are too hard to determine.