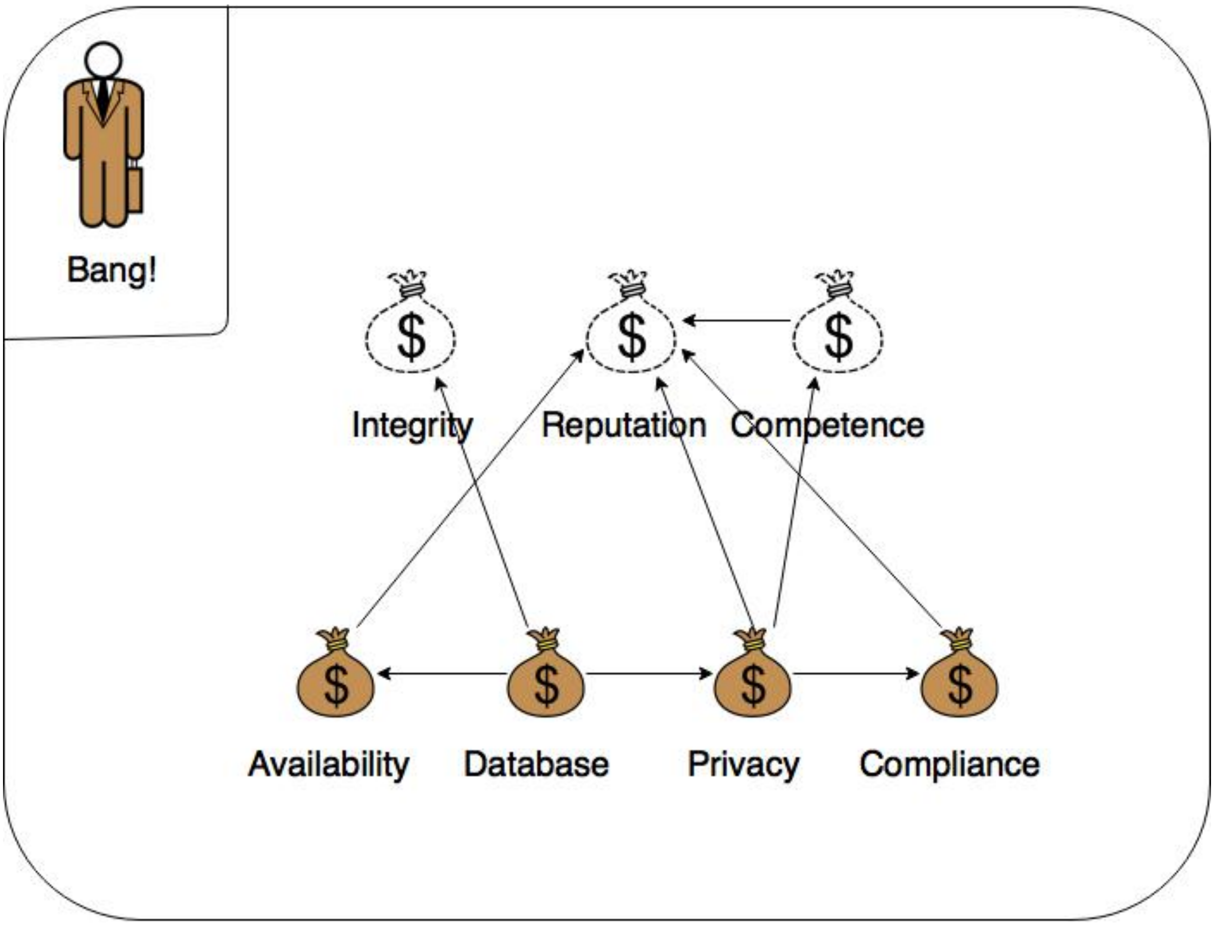
Oblig 3 – Sondre Kristensen

Exercise 1:



Exercise 2:

Who/What?	How, scenario, harm?	What makes it possible?
Hacker	Breaks into system and compromises the integrity or confidentiality of Database.	Remote access to the Recruitment Tool.
System failure	The application is shut down, hurting its availability.	Hardware or software flaws.
Employee	Leakage of private data to the public due to procedural faults, compromising privacy and compliance.	Lack of competence, good procedures.

Exercise 3:

Qualitative consequence scale for the asset reputation

Catastrophic	No one wants to do business with the company
Major	Generally viewed as an unprofessional company
Moderate	Known to have bad practices
Minor	Known to have some issues
Tiny	Disliked by some
Insignificant	Disliked by few

Qualitative consequence scale for the asset competence

Catastrophic	No employee has any idea about what they are doing
Major	Few employees have any idea about what they are doing
Moderate	High up employees lack most knowledge
Minor	High up employees lack some knowledge
Tiny	Some employees lack some knowledge
Insignificant	Few employees lack some knowledge

Quantitative consequence scale for the asset availability

Catastrophic	Unavailable: [1 week, ∞⟩
Major	Unavailable: [1 day, 1 week⟩
Moderate	Unavailable: [1 hour, 1day⟩
Minor	Unavailable: [1 min, 1 hour⟩
Tiny	Unavailable: [10 sec, 1 min⟩
Insignificant	Unavailable: [0, 10 sec⟩

Quantitative consequence scale for the asset privacy

Catastrophic	[50%, 100%] leaked files
Major	[10%, 50%⟩ leaked files
Moderate	[1%, 10%⟩ leaked files
Minor	[0.1%, 1%⟩ leaked files
Tiny	[0.01%, 0.1%⟩ leaked files
Insignificant	[0%, 0.01%⟩ leaked files

Exercise 5:

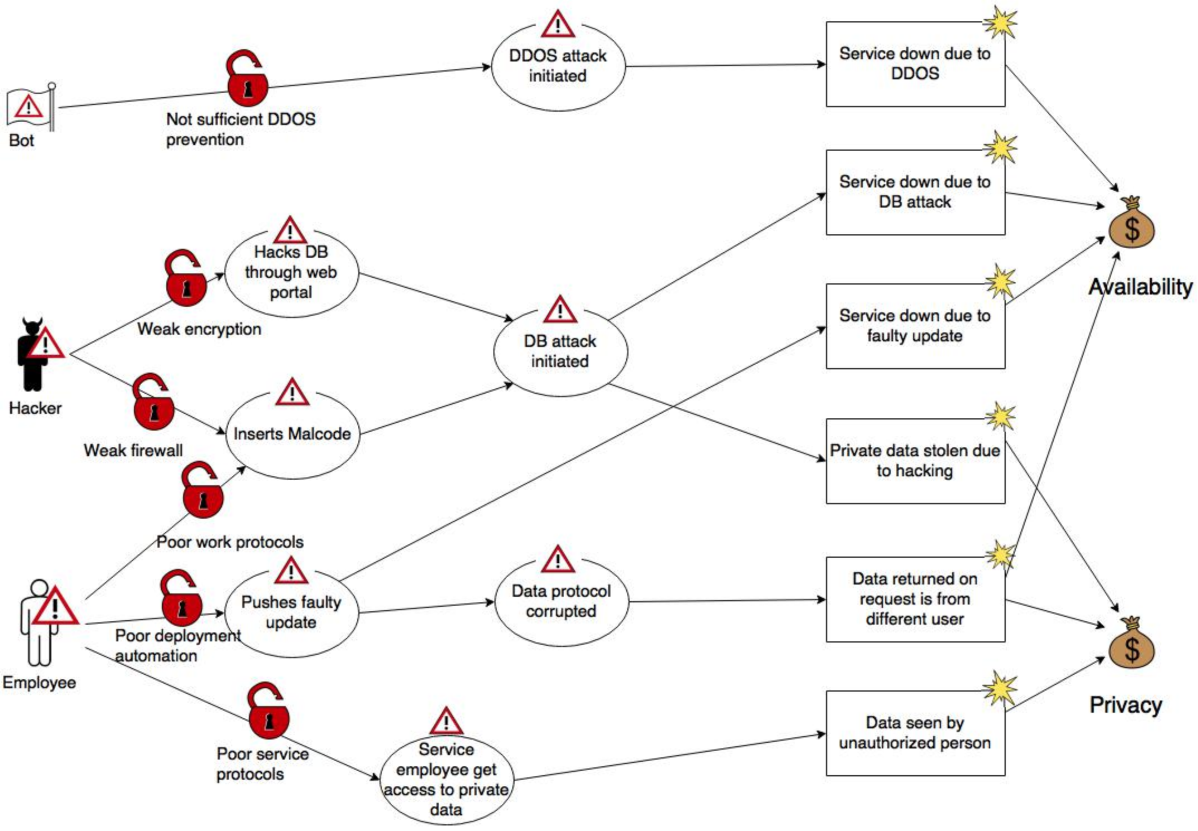
Quantitative likelihood scale

Certain	[100, 1000⟩ : 1 year
Mostly Certain	[50, 100⟩ : 1 year
Likely	[10, 50⟩ : 1 year
Possible	[1, 10⟩ : 1 year
Unlikely	[0.1, 1⟩ : 1 year
Rare	[0, 0.1⟩ : 1 year

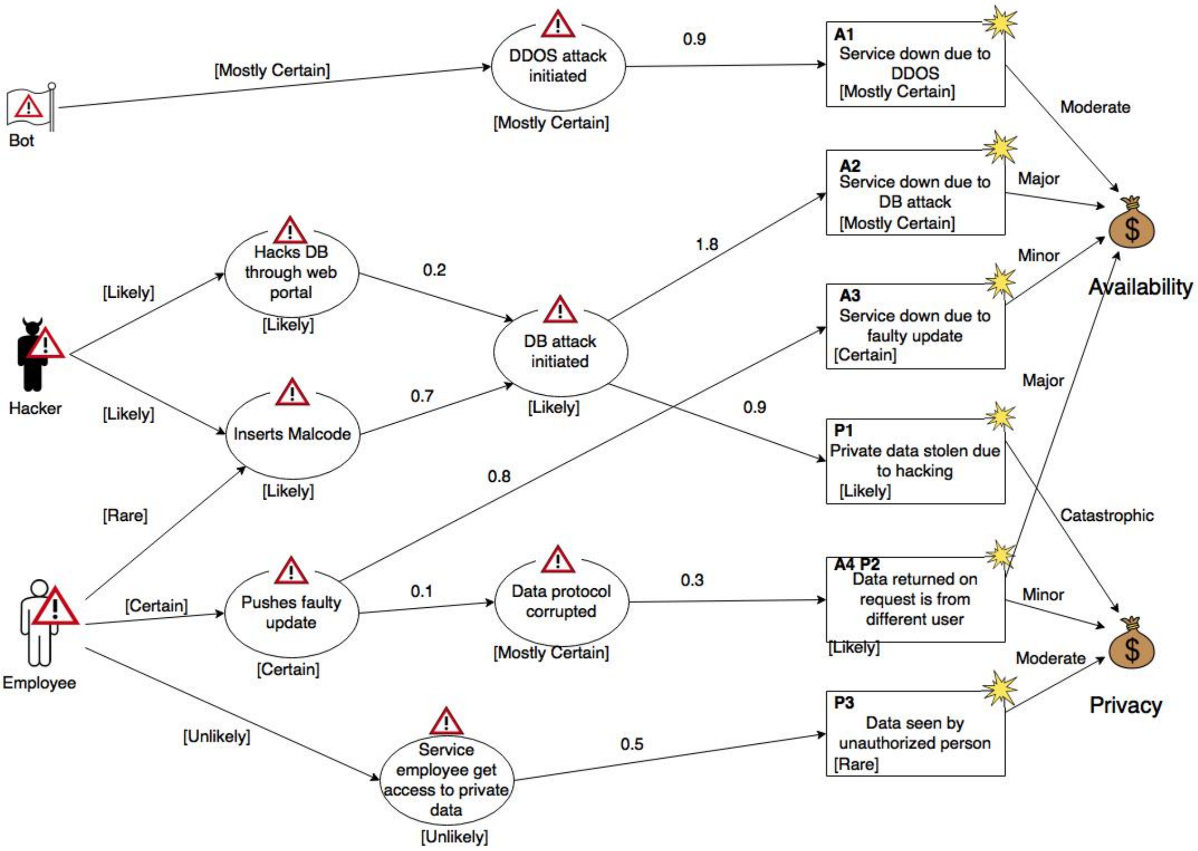
Exercise 4:

Likely/Cons	Insignificant	Tiny	Minor	Moderate	Major	Catastrophic
Rare	🟩	🟩	🟩	🟩	🟨	🟨
Unlikely	🟩	🟩	🟩	🟨	🟨	🟨
Possible	🟩	🟩	🟩	🟨	🟨	🟥
Likely	🟩	🟩	🟨	🟨	🟥	🟥
Mostly Certain	🟩	🟨	🟨	🟥	🟥	🟥
Certain	🟨	🟨	🟥	🟥	🟥	🟥

Exercise 6:


Bot
Not sufficient DDOS prevention
DDOS attack initiated
Service down due to DDOS
Hacker
Weak encryption
Hacks DB through web portal
Weak firewall
Inserts Malcode
DB attack initiated
Service down due to DB attack
Service down due to faulty update
Private data stolen due to hacking
Availability
Employee
Poor work protocols
Poor deployment automation
Pushes faulty update
Data protocol corrupted
Data returned on request is from different user
Poor service protocols
Service employee get access to private data
Data seen by unauthorized person
Privacy

Exercise 7:



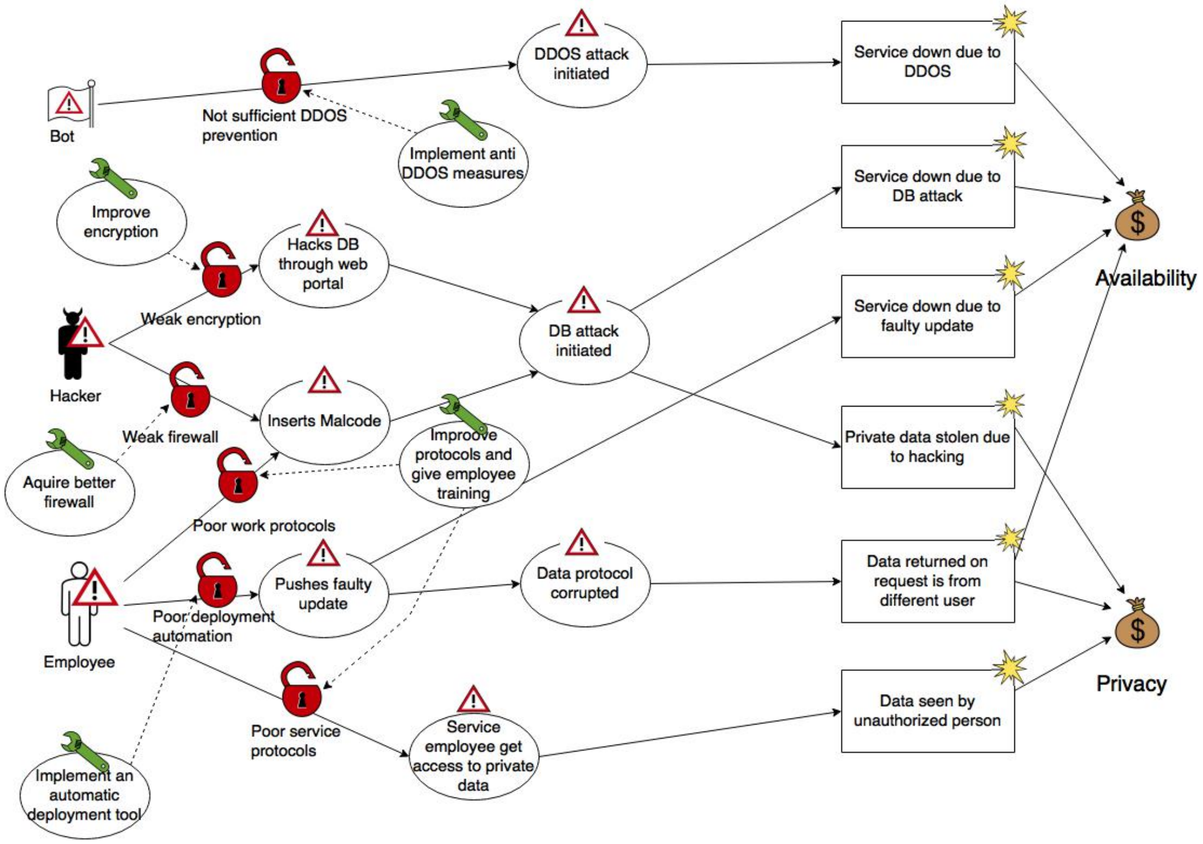
Given that this diagram is complete and there are no other treats that could execute one of the unwanted incidents or threat-scenarios in this diagram, I would argue that this diagram is fairly consistent. Since the likelihood is based on scales, the resulting likelihoods are based on an estimate of which category the resulting interval would belong to.

Exercise 8:

Risk for Reputation	**Based on Direct risk**	**Value**
R1	A1	Mostly Certain, Minor
R2	A2	Mostly Certain, Moderate
R3	A3	Certain, Insignificant
R4	P1	Likely, Catastrophic
R5	A4, P2	Likely, Moderate
R6	P3	Rare, Moderate

Likely/Cons	Insignificant	Tiny	Minor	Moderate	Major	Catastrophic
Rare	🟩	🟩	🟩	P3, R6	🟨	🟨
Unlikely	🟩	🟩	🟩	🟨	🟨	🟨
Possible	🟩	🟩	🟩	🟨	🟨	🟥
Likely	🟩	🟩	P2	R5	A4	P1, R4
Mostly Certain	🟩	🟨	R1	A1, R2	A2	🟥
Certain	R3	🟨	A3	🟥	🟥	🟥

Exercise 9:


Bot
Not sufficient DDOS prevention
DDOS attack initiated
Service down due to DDOS
Implement anti DDOS measures
Improve encryption
Hacks DB through web portal
Service down due to DB attack
Weak encryption
DB attack initiated
Service down due to faulty update
Availability
Hacker
Inserts Malcode
Weak firewall
Improove protocols and give employee training
Private data stolen due to hacking
Aquire better firewall
Poor work protocols
Pushes faulty update
Data protocol corrupted
Data returned on request is from different user
Employee
Poor deployment automation
Privacy
Poor service protocols
Service employee get access to private data
Data seen by unauthorized person
Implement an automatic deployment tool

Some new risks might be introduced due to the introduction of the treatments. For example, the DDOS measures might think a regular employee is trying to do a DDOS attack, when in reality he is just trying to acquire a lot of data, thus sending a lot of request.
The automatic deployment tool might be bugged, and upload some code it is not supposed to do, or some employees might accidentally override the automatic deployment process.