Question 1

Safety

In the context of computer systems and networks, safety has the goal of protecting them against natural risks of its environment and consequences of a risk. That is, not against malicious actions of other actors, such as other computer systems or people. Examples of natural risks are flood, fire, or earthquake. Even if a computer system (e.g. in a data center) is not directly affected by an earthquake, its consequences could be a power failure.

Security

On the other hand, security aims to protect systems and networks against intentional (malicious) interactions/attacks by humans or other computer systems. The focus is on protecting data from unauthorized access and manipulations, and systems and networks from manipulation by, for example, code injections. Security measures must be implemented at all related levels to ensure the highest level of security, e.g., in software, hardware, operating systems, etc.

Question 2

Situation 1

Imitate an existing website (bank, social media) used by a targeted user and get them to enter their credentials.

Situation 2

For example, trick the user with a phishing email to install a malware by opening a malicious attachment.

Situation 3

The attacker impersonates another person (CEO, employee) and gets a user to compromise sensitive company data.

Question 3

Symptomatic

Symptomatic measures focus on correcting the symptoms of a security problem. They respond to an incident and do not proactively prevent the cause(s) of the problem. E.g.: - Having a backup helps to recover from a data loss but not to prevent it to happen in first place. - A sticker over a webcam prevents spying, but not the malware infection itself

Curative

These measures address the root cause of the problems and actively try to prevent incidents from occurring. However, they are not helpful if an attack was nevertheless successful. Therefore, a combination of both concepts is recommended. Eg: - Patchmanagement helps to close public vulnerabilities - Usage of safe programming techniques, like clean coding or pair-programming - Pentests and regulary vulnerability scans

Question 4

IT Security can be improved through IT forensic investigations and techniques by different ways. For example, by analyzing and learning from past security incidents, (unknown) exploited vulnerabilities can be discovered and closed. In addition, the techniques used and the attackers' modus operandi could be studied in order to develop appropriate proactive countermeasures and security strategies.

Question 5

Different topics/examples: ## Data breach Abuse IoT devices as covert channel to extract sensitive business data.

Malware

Connecting a large number of IoT devices together and form a massive botnet.

Physical damage

Manipulation of sensors in critical infrastructures and damage e.g. the power supply of a city.

Financial damage

Manipulation of actors in factory machines and production of inferior products, which can lead to financial loss (e.g. legal actions from suppliers).

Question 6

Cyberwar refers to the use of technology to attack/protect computer systems and networks against other (hostile) states. Thus, IT security impacts cyberwar by protecting systems from such attacks. It is an arms race between the two sides: Each side is trying to stay one step ahead of the other, developing new attacks and defensive techniques.