Exercise: Who is responsible for Mat Honan's attack?
Mat
Twitter
Google
Apple / me.com
Amazon
Whois
Attacker

Who is most responsible?
Attacker takes advantage of holes in Amazon, Apple, and Google, and Twitter. Mat Honan's only responsibility is that all of these are available together, which most people's online presence will be available together.

https://www.wired.com/2012/08/apple-amazon-mat-honan-hacking/

CIA

Confidentiality, Integrity, Availability - the holy trinity of cybersecurity
Authenticity - determining the origin of data - did that person send the email?
Non-Repudiation - proving the integrity and origin

Acceptable Level of Risk: Security has a cost - approximately 20% of the project (generally). Security requires a lot of money to secure something, most companies are only willing to pay a certain amount. There will always be risk

Risk Analysis and Management

Risk = something of value which may lose value if a negative event occurs
Threat = any potential occurrence, malicious or otherwise, that can have an adverse effect on the assets and resources associated with the system
Vulnerability = some characteristic that makes it possible for a threat to occur
Attack/Exploits = some action that involves exploitation of some vulnerability in order to cause an existing threat to occur

Exercise #2

Give an example of threats, risk, vulnerabilities, and exploits
Threat: Disgruntled employee who wants to sell company secrets
Vulnerability: Weak encryption

Risk: The fallout of a successful phishing attack
Attack/Exploit: SQL injection

Treating a risk:
Risk Avoidance
Risk mitigation
Risk transfer
Risk acceptance

Asset Owner vs IT Asset at Risk Owner
The owner of the asset may not be the owner of the related IT asset at risk
ex: an identity that may be stolen is an asset of that person, but the related IT asset is under the control of many other entities
If the owner of the IT system does not suffer the impact of a compromise, what is the motivation to pay for the needed controls for proper risk management?
-Example: Target was breached by hackers between Nov 27 – mid-Dec and personal information for 70-110 million people were stolen. The potential impact of each compromise was on the credit card holders (fraud, identity theft), Target, and the credit/debit card companies (which cover all fraudulent transactions above $50 per account by law).
• Laws and policies are required so owners of IT assets include it in their risk analysis and risk management

Exercise #3:
What would you put as the risk and residual risk of the following:
a: An employee loses a laptop with customer data at the airport. Answer: (likelihood, consequence)
b. How would you mitigate it? Free text
c. What's the residual risk? Answer: (likelihood, consequence)

a. (3, 4)
b. Backup data, device tracking, full disk encryption
c. (3, 2)

Exercise #4:
What would you put as the risk and residual risk of the following:
An executive loses a thin-book laptop with customer data (Name, Full SSN, birthday, address) at the airport. Trudy is actively trying to steal company laptops. The laptop uses full-disk encryption, a BIOS password, and requires an RSA token to unlock. How would you mitigate it? What's the residual risk?

Exercise #5:
Good cybersecurity news

Exercise A:
Explain the difference between quantitative and qualitative risk assessments - provide an example of when you would use each type. Limit your response to no more than 100 words.