Computer/Network Security: focused on preventing undesired behavior

Security Mindset: Thinking of what the system is designed to do and what the proper operation of the system. Thinking of the vulnerabilities, and how it can be defended. Thinking of the cost of defense.

CIA - Confidentiality, Integrity, Availability
Confidentiality: prevent unauthorized reading of information
Integrity: prevent unauthorized changing of information
Availability: Data is available in a timely manner when needed

Risk Analysis and Management
Risk: something of value (asset) that may lose value if a negative event occurs
Threat: any potential occurrence, malicious or otherwise, that can have an adverse effect on the assets/resources associated with the system
Vulnerability: some characteristic that makes it possible for a threat to occur
Attack/Exploit: some actin that involves exploitation of some vulnerability to cause an existing threat to occur

Risk Analysis: Identifying assets, putting quantitative or qualitative measures on the likelihood of the event happening, putting quantitative or qualitiative measures on the consequences of the potential loss

Risk Management:
Risk Avoidance: avoiding the risk
Risk Mitigation: minimizing the potential impact of the risk
Risk Transfer: transferring the risk to another party
Risk Acceptance: Risk is low but costly to mitigate - worth accepting. Monitor

Quantitative:
Exposure Factor (EF) = Percentage of asset loss caused by identified threat
Single Loss Expectancy (SLE) = asset value X Exposure Factor
Annualized Rate of Occurrence (ARO) = Estimated frequency a threat will occur within a year
Annualized Loss Expectancy (ALE) = SLE x ARO

Mat Honan Attack:

- Attacker's goal was to take control of the Twitter handle @mat
- Chose not to attack Twitter authentication directly
- Found personal homepage linked on Mat’s Twitter profile
- Discovered victim’s Gmail address on the homepage

- Visited Google account recovery page
- Recovery page revealed an alternate email ending in @me.com
- Attacker knew @me.com email could be recovered using billing address and last four digits of credit card
- Attacker exploited a loophole in Amazon to get this information
- Called Amazon claiming to be the account holder and requested to add a new credit card
- Only needed email and billing address (found via domain name registration)
- Called Amazon again, claimed email access was lost, and provided name, billing address, and the new credit card number
- Amazon allowed account recovery and sent account info to attacker's email
- Attacker accessed Amazon account and viewed the last four digits of the original credit card
- Used that info to recover the @me.com and iCloud account
- Since @me.com was a recovery email for Gmail and Twitter, attacker also took over those accounts
- Remotely wiped the victim’s computer using iCloud's remote wipe feature
- Demonstrates how different systems' recovery processes can be chained together and exploited