6.9: Summary

6.9.1: Summary

People, businesses, and even nations can all fall victim to cyberattacks. There are different types of attackers, including amateurs attacking for fun and prestige, hacktivists hacking for a political cause, and professional hackers attacking for profit. Besides, nations that attack other nations to gain an economic advantage by intellectual property theft or harm or destroy another country's properties. The vulnerable networks are PC and server business networks and the thousands of computers on the Internet of Things.

Fight against cyberattacks requires people, processes, and technology to follow best practices and good security policies. There are tools that users can employ to protect personally identifiable information. There are policies that companies can require of their customers and employees to protect their resources. Companies can also invest in dedicated Security Operations Centers (SOCs) for cybercrime prevention, identification, and response.

The human element is also a major factor in security incidents. With social engineering and insider risks, no organization can rely solely on technology. A strong security culture with training, leadership buy-in, and thoughtful hiring is key. Investment in around-the-clock security operations centers also enhances threat monitoring and response capabilities.

Finding the right balance between security, usability, and availability allows organizations to implement effective defenses while still furthering business goals. With vigilant governance and coordination between security staff, management, employees, and technical controls, companies can build resilience against today's ever-evolving cyber risks.
