**1. Why is risk assessment essential in cybersecurity? Discuss how it impacts the overall security strategy of an organization.**

Risk assessment is essential to safeguard sensitive data, identify assets, threats, and vulnerabilities, and implement effective mitigation strategies.

Risk assessment is necessary to monitor available resources, prepare for unforeseen disasters, protect data, analyze impact, and prioritize the processes needed to mitigate threats and vulnerabilities. In short, risk assessment helps identify weaknesses and various threats to an organization. By conducting risk assessments, organizations can reduce the likelihood of negative events.

Risk assessments are crucial for an organization. They help in patching the system and network, which is vital for identifying software and hardware vulnerabilities. They also educate end users on the tactics used by threat actors, increasing awareness and reducing susceptibility to common attacks like phishing. Ultimately, risk assessments help organizations prepare for potential risks efficiently and provide countermeasures in the event of an incident.

Regular policy reviews and audits help organizations maintain a strong cybersecurity posture and meet common standards such as ISO 2700, PCI DSS, and GRC compliance. This not only safeguards customer confidentiality but also protects against financial losses that might occur due to inadequate risk assessment.

**2. What are the key steps involved in conducting a risk assessment? Choose one step and explain its significance in the process.**

The key steps involved in conducting a risk assessment are as follow:

- Identify assets  
- Identify threats and vulnerabilities  
- Assess the impact  
- Analyze the likelihood  
- Evaluate existing controls  
- Determine risk levels  
- Develop and implement risk mitigation strategies  
- Monitor and review

**Significance of ‘Monitor & Review’ process:**

The threat landscape and scope of security breaches continue to evolve. With advancements in AI, the tools used by hackers are becoming more sophisticated. Therefore, it is crucial to stay updated on common threats, system upgrades, and education for cybersecurity professionals. Monitoring plays a vital role in ensuring that we stay current and that the infrastructure is resilient to recent threats. The review process helps adhere to the correct frameworks and industry-standard protocols such as those from NIST and MITRE ATT&CK. This is crucial for preparing countermeasures and being proactive in mitigating future cyber incidents, which includes periodically reviewing assets, threats, vulnerabilities, and risk assessments.

**3. What challenges might an organization face when conducting a risk assessment? Propose strategies to overcome these challenges.**

One of the challenges that make it difficult for an organization to maintain foolproof security is the insider threat. This threat comes from within the organization, such as employees, contractors, business partners, or anyone directly related to the business. The impact of such threats can range from stealing a corporate hard drive to ransomware demands for financial benefits.

Some solutions include implementing systems that continuously monitor data usage by end users. Anomalous data transfers (uploads or downloads) should be flagged and followed by risk analysis. Monitoring user behavior, tagging employees with geolocation data, and conducting periodic background checks can help mitigate the impact of insider threats. Additionally, utilizing past cyber incidents caused by human error and providing least privilege access to users can ensure unauthorized data is not accessed.

**4. Share an example of a cybersecurity incident that could have been mitigated or prevented with a thorough risk assessment. How would the risk assessment have made a difference?**

An example is a cybersecurity incident involving a woman in Rochester, where a scammer charged $80,000 on her credit card and transferred $40,000 from her checking account. This started with a phishing email she received on her work laptop.

This could have been prevented through risk assessment by educating end users on phishing, vishing, and smishing attacks. Scammers constantly find new ways to fool people and appear legitimate.

Continuous monitoring of user clicks on URLs is essential. Since this involved a work laptop, any malicious or suspicious-looking emails should have been blocked by mechanisms such as antivirus software or mailing policies.

Conducting risk assessments to identify which departments receive more phishing emails and investigating patterns would be beneficial. For example, the phishing emails received by the human resources department would differ from those targeting the IT department. This incident underscores the importance of risk assessment in protecting businesses and individuals from financial exploitation.