Case Study:1
Sam's Scoop: Vulnerabilities - Threats, Types of attacks and mitigation

Plausible online threats: Phishing, Denial of service attacks, Ransomware.

Threat 1: Social Engineering

Phishing- Phishing is a social engineering technique used by attackers to get confidential information from people or to get them to install malware using suspicious links. A phishing attack could lead to losing confidential information about employees or customers. This can damage the company's reputation and lead to financial repercussions.
Risks associated: Malware
Mitigation: Situational awareness training, email filtering etc

Threat 2: Service Disruption

Denial of Service attacks- Denial of service attacks happen when a server is bombarded with a concentrated amount of unnecessary data requests resulting in it becoming unresponsive. This is usually done with malicious intent, so the server can't respond to legitimate requests which could disrupt the company's operations.
Risks associated: Loss of operations
Mitigation: Firewall, Fault tolerant architecture

Threat 3:

Ransomware- Ransomware is an attack by a threat actor that is caused by installing malware on an organization's network that locks out everyone from accessing critical information until a ransom is paid.
Risk associated: Brute force attack
Mitigation: Strong password policy, removable media policy