While diving into threats, risks, and mitigations, it's clear that infrastructure protection is essential for cybersecurity. The following are some crucial considerations I decided to highlight:

Threats:

- Malware is a major threat where malicious software can attack computers and damage them or steal private information
  - Some relevant tools are Ransomware, viruses, and Trojans
- Social engineering is the practice of tricking people into disclosing private information or taking actions that could jeopardize the security of a system
  - Phishing, pretexting, and baiting are a few examples
  - Similarly inside threats occur when employees of a company have access to sensitive data or systems and inadvertently or purposefully cause harm
- Attacks that deny users access to a system by overloading it with traffic or requests are known as denial-of-service attacks

Risks:

- Data breaches were a repetitive risk I saw and often led to the loss of private information, having detrimental effects on both people and organizations
- Downtimes were a risk which affected a system's and service's accessibility, resulting in lost productivity, lost revenue, and reputational harm
- Legal and regulatory compliance revolves mostly around violations of the law which is addressed in the capstone PDF

Mitigations:

- Firewalls are a great mitigation tactic which can watch and filter both incoming and outgoing traffic, obstructing harmful traffic
- Antivirus softwares are decent at identifying and removing malware from systems, this software helps to shield them from harm and data loss
- Encryptions upon doing further research, including the segment diving into cryptography through the Security+program, in short lowers the risk of data loss or theft by converting sensitive data into a coded format that can only be read with the proper decryption key
- Access controls can restrict who has access to private systems and information, lowering the possibility of insider threats and unauthorized access
- Planning for disaster recovery is basically where you develop processes and procedures for restoring systems and data in the event of a significant interruption or outage

The general takeaway from my research is that safeguarding infrastructure entails a variety of factors, such as comprehending the various risks and threats present and putting in place efficient mitigations to lessen these risks. With this, organizations can guarantee the safety and security of their digital assets and shield themselves from potential harm and reputational damage by adopting a strong approach to cybersecurity.