Risk Assessment Report for TechCorp

Summary of Identified Risks

A comprehensive risk assessment was conducted to identify potential risks to TechCorp's assets, including customer data, servers, applications, and employee personal data. The following risks were identified:

- Malware infection

- Data breaches

- Phishing attacks

- Insider threat

- Physical theft of devices

Risk Matrix

The risk matrix below visualizes the likelihood versus impact of each identified risk:

Likelihood (Low, Medium, High) vs. Impact (Minimal, Moderate, Severe)

| | Minimal | Moderate | Severe |

| --- | --- | --- | --- |

| Low | Insider threat | | |

| Medium | Physical theft of devices, Phishing attacks | | |

| High | | | Malware infection, Data breaches |

Key Recommendations

To mitigate the top risks, the following key recommendations are proposed:

1. Implement robust antivirus software and employee training to prevent malware infections.

2. Enforce access controls, including multi-factor authentication, to prevent data breaches.

3. Regularly back up critical data and store it securely to minimize the impact of potential data breaches.

By implementing these recommendations, TechCorp can significantly reduce the likelihood and impact of malware infections and data breaches, protecting its valuable assets and maintaining a secure and resilient digital environment.