Risks:

1. Compromisation of network
2. Physical hardware failures
3. Employee data leaks
4. Data manipulation
5. System Maintenance
6. Data recovery

Risk	Probability of Loss	Size of Loss	Risk Exposure
Compromisation of network	Unlikely	Major	High Risk
Physical hardware failures	Unlikely	Major	High Risk
Employee data leaks	Moderate	Catastrophic	Extreme Risk
Data manipulation	Moderate	Moderate	Moderate Risk
System Maintenance	Moderate	Moderate	Minor Risk
Data recovery	Rare	Moderate	Minor Risk

Top 2 Risks:

Risk	Risk Response
Compromisation of the network	**Buy Information:** Completely understand how the system works and how what information we can obtain to keep the network protected. **Mitigate:** To reduce the probability of unwanted access, we would do penetration testing to exploit any weaknesses that we may find on the network.

	Accept: We accept the risk and make a contingency plan to assess the vulnerabilities in our network. The plan will contain ways on how we can recover if the network were to be shut down.
Physical hardware failures	**Avoid:** To avoid physical hardware failures, we would ensure updates and regularly scheduled maintenance to both the hardware and system. Proper use and quality of the hardware will help prevent failure. **Mitigate:** Quickly identify the problem and determine the most efficient solution. Proceed to develop proper documentation regarding the specific problem in case the problem arises in the future. **Accept:** We accept the failure and get replacement equipment for our network/systems. We restore our systems back to a functioning state with backups.