Deliverable 1:

1. There are many risks with allowing employees to access work information on their personal devices. Some are data leakage, lack of management and installing sketchy apps on the device. There can be phishing attacks on these devices, malware and other viruses can be installed and run in back that steal valuable company information, and these devices can also get stolen easier. All of these are detrimental to the company.

2. App segregation that creates a barrier between personal and private use can mitigate the risk of the wrong access to files. Using a VPN would help to protect from network interception. Integrity monitoring can show if negative changes happen to company files and can be corrected quickly.

3. You could send out test emails to see if employees are easily fooled into clicking the wrong things, which could potentially be phishing email attachments, etc. After, create a graph on who clicked and who didn't, and retest a week or so later.

4. The goal would be just that. To get a very low number of employees clicking the wrong things, and understand how easy it can be to be fooled into something so quickly. You want to make sure employees are paying attention in meetings on how to reduce the risk of the company's data from being accessed by the outside world.

Deliverable 2:

1. Network Security Team. They would be responsible for changing passwords once a month to appropriate passwords that aren't guessable. They would also be the ones responsible for conducting quarterly assessments or reviews on employees to ensure they are not risks to the company. Also, for installing VPN's and monitoring network traffic. They need to make sure the risk of attacks is low, and have a plan ready to execute if the network does get taken down, in order to bring it back up with the least down time possible.

2. Managers. They would be responsible for hiring the correct people, and at the same time getting rid of malicious employees. They are also responsible for reporting to the administrators their reviews of employees and make sure their employees have the correct training and resources. Also, risk management is necessary in order to mitigate risk.

3. Administrators. They would work above or alongside the Network Security Team. It would be their responsibility to ensure a hot server is in place. This way they could bring the network back up very quickly if it were to go down or get hit by a DDoS attack.

4. Auditing team. They would perform audit-only tasks. Thoroughly evaluating employees performance and work. If someone is suspected to be a malicious employee this department would evaluate them.

5. Physical Security Team. They would be responsible for having a guard at all entry points at all times. Also, they would be responsible for any finger print scanners, eye scanners, security camera monitoring, etc. They could also install a turnstile and have people that aren't employees go thru a check-in process.

Deliverable 3:

We would run training quarterly. There would be cybersecurity training and an unexpected test after to monitor the results. We would cover everything from phishing emails to how holding the door for

someone at the entrance point could be risky. How to create safer passwords, not to share passwords or company info with others, and how downloading things that aren't necessary for work can also be a very big problem. We could also go over some examples of data breaches that have happened in the past, so it gives everyone a better idea of how realistic these threats really are. The test afterward would measure the effectiveness.

Deliverable 4:

Hot Server. Technical control. This would be a combination of preventative and corrective. The goal is to mitigate the risk of network breaches and unauthorized people from accessing the building and network. If however, this is to fail, it is important to have a plan in place to be able to recover as quickly as possible to have the least minutes down. A hot server on backup ensures a fast recovery.

24/7 Security Guards. This is preventative and detective. It will keep a close monitor on who enters and exits the building. If they notice something suspicious, they can take note of it and take the necessary measures to stop/prevent it.