2-2 Project One Stepping Stone One: Risk Register

Joshua Merren

Southern New Hampshire University

CYB-410-13417-M01 Security Risk Management

Professor Christopher Molstad

11 September 2024

The first risk I selected is the technology risk, especially the chance of our point-of-sale (POS) system going down. This could lead to major disruptions in sales and cause significant downtime. I identified this risk because the POS system is critical for keeping track of all our sales. Without it, we might lose important data and even need to close the shop temporarily until everything is back up and running. I rated the probability as moderate because even though it does not always happen, power outages or technical issues are still possible. The impact is also moderate because the seriousness depends on how long the system is down. If it's only a few hours, it would not be too damaging, but if it lasts for days, the financial impact could be significant. Without action, we could lose customer records and sales information, forcing us to rely on paper and making things more challenging to track. The best time to act would be as soon as we notice the system starting to fail. We can call IT support right away to avoid more extended downtime. We may access the POS system with a backup laptop ready to go. Doing so could help us keep operating while IT fixes the primary system. I would expect IT support to handle the situation effectively since they know our system well, and they should be able to restore everything quickly, syncing it back with the cloud to recover any lost data.

The second risk I chose is related to physical security. The concern is the possibility of a break-in if our cameras stop working due to an internet outage. Our camera system depends on the internet and cloud storage, so if either goes down, we lose access to live footage and stored recordings. This could be a problem if something happened, like a break-in, while the cameras were offline. I rated the probability of this happening as low because internet outages are rare, but the impact would be medium since the consequences depend on the timing. If there had been no break-in during the outage, it would not have been too harmful, but if something had happened, we would not have had any footage to help track down the culprit. The right moment

to respond would be when the cameras are not syncing with the cloud. At this point, we would call IT support or the camera company to troubleshoot the issue and get the system back online. In the worst-case scenario, the camera company could send a replacement if it cannot be settled remotely. After contacting support, I expect they would be able to troubleshoot and resolve the issue quickly, ensuring the cameras are functioning correctly again and synced to the cloud, so we don’t have any gaps in our security footage.