Moho’s Network Security Defense Company for Groceries

By: Mohanad Horani

NTS415

(360 Smart Networks, 2021)

Where are We Located?

- Our company is located in the city of San Francisco in the state of California. The reason we chose this specific state is since it is a large state. A large state means more access to resources needed to help the company as well as being able to hire more employees for our company as well.

What Do We Do?

- The answer to the above question is that Moho’s Network Security Defense Company for Groceries helps protect grocery stores from having any breaches and hacks. In other words, our purpose is to defend grocery stores in the city of San Francisco from being hacked. Also, our goal is to monitor the security cameras inside of the grocery stores from being hacked as well by monitoring the cameras daily for any unusual customers or employees (i.e. suspects).

What Assets are We Trying to Protect?

- Employees in Grocery Stores
- Security Cameras in Grocery Stores (i.e. from being hacked).
- Valuable Data that may be stolen if not protected
- The Customers inside of the Grocery Stores
- Our own employees in the company
- Technology in our company
- Data in our company.
- The items inside of grocery stories (i.e. Protecting groceries from being stolen)
- The WiFi networks that run inside of the grocery stores in the city of San Francisco and our own Wi-Fi as well especially.

Risks

- 3 Risks include the following:
  - Computer viruses in the employees’ computers
  - Untrained employees for our company which means our company may be bankrupt in the future if people cannot perform their jobs properly.
  - Software Vulnerabilities

3 Policies to Cover the 3 Risks

- Policy #1- In order to protect the computers from computer viruses, simply install antivirus software and make sure a firewall is on the network. Not only that, make sure only authorized employees are allowed on the computers in the workstation.
- Policy #2- Have a hard policy about logging off each time an employee is done with the workstation. Not only that, make sure no foods or drinks are allowed near the workstation and monitor employees that are beginners in their area from time to time. This will fix the issue of employees who may not be trained and are breaking rules on purpose which can then lead to possible future removal.
- Policy #3- In order to fix software vulnerabilities, simply file a bug report to the appropriate individuals depending on which software company has the issue. Then, have the employees immediately notify the manager of the software vulnerability they encountered.

References

- 360 Smart Networks. (2021, February 2). *Cyber security in Atlanta & Charlotte – IT services company*. https://www.360smartnetworks.com/cyber-security-in-atlanta/