

One disastrous attack that I had thought about were individuals using keyloggers to retrieve passwords from employees through phishing emails. I vision that they intruders would make a phishing email similar to a company that you might partner with. The hackers would most likely retrieve any information from the company that could be valuable to them . This could potentially lead to the downfall of the company's reputation. The people that this cyber attack could affect would be the employees within the company. If the hackers were able to get ahold of the employees information, then they could possibly see their social security numbers, homes and addresses and lead to stealing identities.

The cyber attack would most likely shut down all the systems that the employees use for work. This would cause the company to lose any data that was not saved in an external storage or in the cloud. A lot of the computer systems would be affected because, if your company is solely based on technology, then having a breach or attack like this causing the company to spend more money on securing networks and hardware systems than actually focusing on the main job itself. Many of the employees would be affected because they might feel as if their privacy or personal information cannot be maintained in the company, causing many of the employees to quit due to the lack of security protocols. There are many possible ways that the cyber attack could have been prevented. The first one

could be by assuring all your employees are aware of what phishing emails look like, and how to handle it if you suspect one. Another way, is by ensuring that you are monitoring your system and any traffic that is coming through.