t

Group Assignment #3

[Group 10: Jessica Pham, Justine Lam, Jiajun Gu, Zack Nguyen, Ben Kwok]

# Question 1:

A screenshot of a cell phone

Description automatically generated

Consider the categories of threat in Figure 10-3. Describe the three most serious threats to each of the following businesses:

1. A neighborhood accounting firm
   1. Incorrect data modification — Natural disasters: Natural disasters are extremely devastating and in turn if the data is incorrectly recovered, a neighborhood accounting firm can suffer great consequences. Unlike a large accounting firm with greater quality systems that are more likely better equipped to handle and resolve situations like this, a neighborhood accounting firm will likely not be able to recover from a damage like this. Rather, this accounting firm may lose its business from the neighborhood for not being able to correctly operate for a small group of people.
   2. Unauthorized data disclosure — Computer crime: Unauthorized data disclosure from a computer crime creates many problems not only amongst the neighborhood accounting firm itself, but its customers as well. A breach of data is extremely difficult to recover from, the accounting firm can lose precious data and business if the data is in the wrong hands and leaks to other competitive firms. Hackers can pre-text the customers and scam them in multiple ways, including leaving that firm into a fake one where the hackers can continue stealing from them.
   3. Faulty service — Human error: Faulty service caused by human error such as procedural mistakes and/or development and installation errors can cause serious mix-ups within the accounting firm’s system. These mistakes can be costly, especially if the mistakes were from installation problems because then the system is prone to always creating inaccurate files and data which is problematic for an accounting firm because it deals with money.
2. A Dentist's office
   1. Denial of service — Natural disasters: A natural disaster can lead to the denial of service at a dentist office because depending on how severe the disaster is, employees of the office may need time off in order to recover, resulting in service interruption because they will not be available to work on/help patients.
   2. Faulty service — Computer crime: Just like every other medical clinic and offices, dental offices must also abide by HIPPA. A computer crime that causes faulty service can lead to a leak of patient information that is supposed to remain confidential. This can lead to usurpation and all the information that is obtained can be used against the dental practice and patients themselves.
   3. Incorrect data modification — Human error: Incorrect data modification by human error can be damaging to a dentist’s office because incorrect entry of information can create many problems for the office. Incorrectly inputting a patient’s medical history into a system can cause a deadly lawsuit if this mix-up brings a patient any harm. Incorrect data entry can also create scheduling conflicts which would bring complete chaos into the office.
3. A Honda dealership
   1. Loss of infrastructure — Natural disasters: A natural disaster that causes a Honda dealership to lose its infrastructure would be completely devastating to the dealership. Not only would they lose their property, but also their products, the car. Depending on how severe the natural disaster is, they could completely lose everything their business is focused on selling, meaning they wouldn’t have a business to run then.
   2. Incorrect data modification — Computer crime: Incorrect data modification from a computer crime could lead to hackers creating inaccurate information that could cause the dealership to lose business. Hackers could incorrectly give customers a large discount on a car or upload misinformation on the Honda dealership’s website. Whenever customers are brought into the picture, businesses usually suffer greatly because they lose out on the relationship they may have worked towards which in the end usually means the business loses the customer to another dealership.
   3. Faulty service — Human error: Faulty service caused by human error would make this Honda dealership look very unprofessional, especially if the mistake the employee made was ordering the wrong product. After waiting for weeks to receive a car with their customized ideas and receiving the wrong order may cause their patience to run thin and no longer wanting to return and work with the dealership. Another faulty service human error would be to send the wrong bill to the wrong customer which would cause many mix-ups and frustration.

# Question 2:

Describe a potential technical safeguard for each of the threats you identified in your answer to question 1.

A potential technical safeguard for incorrect data modification would be securing the data into a secure server, while backing up the correct data into a separate, offline server. For unauthorized data disclosure, a potential safeguard would be installing effective firewall policies and anti-virus on the data server to prevent any hackers. For faulty service in human error, a potential technical safeguard would be setting up usernames and passwords for each person, who accesses the data and having access control policies for each person. A potential technical safeguard for denial of service regarding natural disasters would be implementing a back-up plan and providing support and benefits to the employees if needed. For loss of infrastructure, a potential technical safeguard would be constructing the property to prevent major destruction on the business.

# Question 3:

Describe a potential data safeguard for each of the threats you identified in your answer to question 1. If no data safeguard is appropriate to a business, explain why.

Natural disaster: we should back up data periodically in a different place. Also, periodically practice backing up the data just in case everything is correctly operated; Unauthorized data disclosure: we should create multiple strong passwords and use proper encryption; Faulty service: we should have physical security such as locking databases in a secure location to limit damage due to personal fault while having a clear log to record activities. Also, regularly check the accounting statements to figure out errors. Clearly define data rights and policies. In addition, clarify responsibilities related to different situations.

# Question 4:

Describe a potential human safeguard for each of the threats you identified in your answer to question 1.

The company needs to clearly define position and responsibilities while giving proper job descriptions. The company needs to repeatedly train employees for security including fully informing the security policies. Background investigation on sensitive positions is required when hiring. After hiring, the company should apply security screening. The company should have proper account management. For example, remove account and password when an employee is promoted or retired. Ask employees to change passwords frequently. In addition, create a system that does not allow employees to switch back to old passwords.

# Question 5:

Describe how each of the businesses in question 1 should prepare for security incidents.

* Neighborhood’s Accounting Firm
  + The Neighborhood accounting firm should prepare for any potential data breaches that may allow hackers to have access to sensitive information. This is especially important with a small local firm, as those generally have a smaller budget for extra security. They may do this by having a highly recommended and trustworthy server that they can safely store all of their data on.
* Dentist’s Office
  + A Dentist’s Office should prepare for any potential security risks like theft or robberies. This is because these buildings generally hold lots of highly valued equipment as well as medication that people would be likely to steal. In order to prepare for this, security cameras and potentially even security guards would be suitable for such events.
* Honda Dealership
  + A Honda Dealership, or any dealership in general, should obviously have security guards and cameras for the extremely expensive vehicles that they own. They might even want to have trackers on each of their cars, so that people that go on “test drives” don’t steal their vehicles. Another important thing to consider is the information of employees and customers, because generally credit checks are needed for people to finance cars, which will mean that social security numbers and other sensitive information would be needed (and needed to be protected).

# Question 6:

How likely are the threats you identified in question 1? If you owned these businesses, which of the items you described in questions 2 through 5 would you implement?

* Many of the threats that were identified in question 1 are highly unlikely, however it is always preferable to be ready in case any of these security threats were to occur. I would personally implement all of the security measures, from having a secure database, security guards, security cameras, and even having tracking devices for highly valued items. There should always be a strong budget for security purposes, because not only are you risking the company’s information and equipment, but the customers as well.

# Question 7:

1. Explain why Moore’s Law makes it increasingly more important to create strong passwords.

Moore's law is a law that basically says that the processing power of computers has developed quickly and will keep on developing. Accordingly, Password intricacy needs to become similar as quickly as power develops since computer’s processing ability is constantly updated to figure passwords.

1. Do you agree that Moore’s Law is helping the “bad guys” more than the “good guys”? Why or why not? Use evidence in this case, knowledge from this chapter, and your own experience in your answer.

With Moore's law’s principle that speeds up a CPU, hackers can be made easier to crack passwords. By increasing the speed, the hacker can quickly crack the password in a relatively short time. In general, as long as users use strong passwords, this regulation benefits the good guys rather than the bad guys. In Moore's case, Even we know about protecting our computer resources, there are many cases of data breaches that occur today, which will make the cyber criminals' devotion to exploiting whatever flaws exist. We have little knowledge of failed assaults since they are rarely reported. Therefore, it's crucial for individuals and commercial groups to remain careful.