CIST 3381- Information Assurance & Security

Spring 2022

Case Study 3: Cyber Attack at the University of Calgary

Be sure to give detailed responses (Minimum 150 words per question)

Michael Chillemi

Ques 1) A cybersecurity breach exposes an organization to reputational operational and financial

issues. Discuss different issues related to a cybersecurity breach?

During the data breach there was many issues that occurred during the scary event. First of the many issues is that the data became encrypted which made it very hard for them to deal with. Another issue we found was that the IT department was having issues as well as the IT users. They had to shut down the email server. This type of event can cause lots of damage with the staff, student, researchers, doners, and the reputation of the town itself.

Ques 2) Should the University of Calgary pay the ransom?

This answer can go both ways with if they should or shouldn’t pay the ransom. For the reason not to is that they can not guarantee that a future attack will not occur. Also, they have the ability to leave a back door to regain access. It may also damage their reputation more and the keys they give may not work. The reason to pay the ransom is to protect their information. Also, to retrieve crucial information to researchers.

Ques 3) What course of action (during and after the crisis) would you suggest the university take

to communicate with its stakeholders effectively?

During the crisis the university should have informed the stakeholder about the situation when it originally happened. Also, they should alert the head of the departments so they can distribute the same information to the college in that department. Plus mentioning the email severs are down to keep everyone up to date. After the crisis they should find a more secure way to communicate when the email severs are down. Obtain more resources to prevent an attack. Last they should double check the data to verify that it was not tampered with.

Ques 4) U of C researchers could use personal computing equipment to conduct research or use

the U of C's IT resources for personal records and projects. How should prioritization of

recovery and privacy be managed?

The prioritization if the recovery and privacy should be managed by a trusted leader of the university. They should also ensure the privacy and verify that the confidential information or the researchers information was not tampered with.