CIST 3381- Information Assurance & Security
Spring 2022
Case Study 3: Cyber Attack at the University of Calgary

L1
Group Name:

Group members' names:

1. Michael Chillemi
2. Vivian Hin
3. Amanda Quach
4. John Raven

CIST 3381- Information Assurance & Security
Spring 2022
Case Study 3: Cyber Attack at the University of Calgary

Group Name: LZ **Your Name:** Michael Chillemi

Ques 1) A cybersecurity breach exposes an organization to reputational operational and financial issues. Discuss different issues related to a cybersecurity breach?

Answer:

Personal issue
- it department
- it users
- communication
- Data is encrypted
- losing the ability to get data
- [redacted] an trust worthy - with staff
- [redacted] emails
- [redacted] reputation
  - staff - damaged
  - students - donations
  - reserve - town college is ...
- financial issue
  - spending money/resource to control breach
  - pay ransom to unlock computers.
  - does less likely to give school money

CIST 3381- Information Assurance & Security
Spring 2022
Case Study 3: Cyber Attack at the University of Calgary

Group Name: L1 **Your Name:** Vivian Hin

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

Answer:

Reason not to:

- can't guarantee that a future attack won't occur again
- hacker can leave a back door
- the key may not work
- damage reputation
- easy target for new attackers
- used to fund new attacks

Pay the ransom:

- protect information (i.e. personal information, intellectual property, emails, etc.)
- U of C system is down & prevent normal operation
- retrieve data back, crucial for researchers

CIST 3381- Information Assurance & Security
Spring 2022
Case Study 3: Cyber Attack at the University of Calgary

Group Name: L1 **Your Name:** Amanda Quach

Ques 3) **What course of action (during and after the crisis) would you suggest the university take to communicate with its stakeholders effectively?**

Answer:

During: Should inform the stakeholders of the situation.
Tell Department heads so they can inform their department on how to protect their information/data.
Mention email servers are down (Updates on their Social media Twitter)
Accuracy
Consistent

After: Find another more secure/effective way for when email servers are down. to communicate.
Mention types of data compromised.
Update/transparent of the crisis (what was done)
Obtain more resources (funding, hiring, improve infrastructure)
Ways to Prevent the attack again.
Double check data (if everything is working & there)

CIST 3381- Information Assurance & Security
Spring 2022
Case Study 3: Cyber Attack at the University of Calgary

Group Name: L1 Your Name: John Reaver

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?**

Answer: The university should prioritize recovery of UofC issued machines. When users join the network they are asked about the privacy of the network. A university is technically a private network because of accounts being necessary, but it's such a large network that it's still dangerous to allow file sharing on the network. They should disclose that if a personal device was connected to the network during a specific time period of the attack that it may be compromised. The university should not be responsible for ~~on~~ personal computers if the user was offered a university issued device.

Not what the question was asking

Ask leadership who should be prioritized
Proper ~~confi~~ confidentiality necessary for documentation