Cyber – The Changing Battlefield

The story from the front lines

UNIVERSITY OF CALGARY

Janet Stein, Director, Risk Management & Insurance

January 26, 2017

Presentation to the Disaster Recovery Information Exchange

UNIVERSITY OF CALGARY

Ransomware Attack

- Late on Friday, May 27, 2016, the University of Calgary experienced a ransomware malware attack.
- **Ransomware** is a type of malware that severely restricts access to a computer, device or file until a ransom is paid by the user.
- Both applications and files were infected, including one of our major email systems which had over 9,000 users.

UNIVERSITY OF CALGARY

The Response: Boots on the Ground

- Chief Information Officer, Associate VP Risk, VP Finance, Director of Risk Management & Insurance and the Privacy officer were notified.
- Emergency Response Team was convened.
- University Relations handled communications.
- The Cyber and Data Security insurance policy was checked – the "Duties in Event of a Claim" section.
  - The Cyber Breach coach was contacted, retained and engaged.
  - The Security specialists were engaged and on site within a few hours.

UNIVERSITY OF CALGARY

The Response: Breach Containment

- Affected computers/file servers were physically unplugged or virtually "sandboxed".
- Determined that infected equipment in sleep mode was o.k. if not awakened.
- Campus-wide message: "Don't touch your computer".
  - Posters on every external door on campus.
  - IT Website
  - UCEmergency App Notification
- By Monday morning Deloitte had deconstructed the malware and created a "blocker" app and the anti-virus companies had updated the signatures. The blocker prevented the program from executing, malware detection tools and anti-virus wiped it off.

UNIVERSITY OF CALGARY

The Response: Assess Source of the Breach

- Traced the malware – determine where it came in, how it infected the system and then trace the infection (almost like a pandemic diagram).
- Deloitte worked on the "fingerprints" of the ransom tool to try to determine the trail of the originator (i.e. external/internal, country source, chatter on the dark web or the regular internet).
- Retained all the forensic evidence related to the breach (can be required for police or insurance company.
- Documented actions taken – meeting 3 to 4 times a day.

UNIVERSITY OF CALGARY

The Response: Courses of Action

- Determined systems and users affected – suspected or encrypted machines.
- Portals re-evaluated for criticality and behaviour patterns.
- Email was inaccessible for over 8000 people – Provisioned 8,000+ Office 365 email accounts in 5 days.
- Identified events and other activities happening on campus and how they would be impacted.
- Investigated whether personal data could have been breached.
- Network tools enabled for constant monitoring of internal (across the network) and to external (outside to inside the network) activity.
- Addressed equipment beaconing out to the internet and portals allowing suspicious content into the network.

UNIVERSITY OF CALGARY

Ransom Payment – Making the Decision

- Ransom notes normally provide up to 7 days for payment.
- Payments are always in bit-coin.
- Considered whether any information could be on computers that were not backed up and how critical it may be.
- Debated paying the ransom as payment does not guarantee the encryption keys will be released or that the keys themselves could introduce new malware.
- Considered mitigating litigation possibilities arising from un-backed up information through paying ransom.
- Utilized existing Governance structure for making the decision to pay.

UNIVERSITY OF CALGARY

Ransom Payment – Making the Decision

- Ransom paid – 27 bitcoins – ~$20,000 CDN
- Waited for the decryption keys – will they send them?
- Had more than one set of experts "clean" and test the keys.
- UofC went public with the information.
- Continued to monitor systems in case this sparked other attacks.

UNIVERSITY OF CALGARY

Ransom – Public Disclosure

University of Calgary pays hackers $20,000 after ransomware attack

SHAWN LOGAN

More from Shawn Logan

Published on: June 7, 2016 | Last Updated: June 8, 2016 10:22 AM MDT

SHARE

ADJUST

COMMENT

PRINT

The University of Calgary paid a $20,000 ransom in untraceable Bitcoins to shadowy hackers after a devastating malware attack.

Linda Dalgetty, the school's vice-president of finance and services, said the cyberattack that crippled multiple systems on May 28 used so-called ransomware, which locks or encrypts computers and networks until a monetary ransom is paid.

She said officials agreed to pay the ransom to ensure critical systems could be restored, but noted it will take some time for the university's IT staff to apply the encryption keys to the infected machines.

"What happens is you pay the ransom and the bad guys physically provide the keys," Dalgetty said Tuesday, noting more than 100 computers were affected by the virus.

"At this point, we do have some encrypted machines. We have not used any of the decryption keys."

Dalgetty said university IT teams have been working around the clock for more than a week trying to fix the bug that affected email, Skype, wireless networks and other services. Users of university-issued computers were also advised to leave them off while under threat from the hackers.

In order to receive the keys, the school paid the equivalent of $20,000 CDN in Bitcoins, a digital currency considered largely anonymous and untraceable. As of Wednesday, the price in Canadian dollars for one Bitcoin is $739.65.

As for why the U of C admitted it paid the ransom, as well as releasing the cost, Dalgetty said it's an effort to be transparent.

"We're a public sector organization and we pride ourselves on our openness," she said.

UNIVERSITY OF CALGARY

Insurance

- Public relations and crisis management consultant to avert material damage to brands/business operations.
- Forensic consultant to attempt to establish the identity of the hacker.
- Security specialist to assess the electronic security and costs of reasonable security improvement.
- Temporary storage of electronic data at a third party location.
- Privacy data breach cover.
- Cyber extortion cover.
- Cyber business interruption cover.

UNIVERSITY OF CALGARY

What Worked Well

- ERT and IT incident command in place very quickly. Regular meetings. Specific deliverables monitored.
- Engaged specialists.
- Purchased insurance – allowed us to access resources and expertise you don't normally require.
- Cared for the people – ice cream, popcorn, addressing burn-out
- Brought together Institutional Crisis Management Team and Emergency Operations Centre when required.

UNIVERSITY OF CALGARY

What Worked Well

- Provisioned over 8,000 new emails in 5 days to allow people to continue to work.
- Contacted the right people – internally and externally.
- Communicating with the campus – generally positive feedback.
  - Repurposed UCEmergency App for campus communications.
- Kicking it back to the 80's (unplugged)
  - re-connecting with people face-to-face ("sneaker-net").

UNIVERSITY OF CALGARY

What Worked Well

- Brought IT to the people – Created "pop up" IT help centres across campus to facilitate mandatory password change.
- Crisis Response Centre:
  - Levity in the Crisis Room:
    - "Word of the Day" challenge.
  - Continuity of leadership in the room.
  - Constantly re-prioritized worklist to fit the situation; tracked activities and deliverables.
- Publically acknowledged ransom payment.

UNIVERSITY OF CALGARY

What We Do Differently

- Breach Coach and Security Specialists on retainer.
- Restrict full network access to managed devices only – provides visibility of equipment to IT and allows IT to update malware and virus detection software.
- Establish process and rules around decrypting data.
- Recognize that the situation may require significant time to fully resolve.
- Ensure offline contact information is available for key individuals in the institution.

What We Do Differently

Predetermine Who May Need To Know

- Privacy Officer (in case there is a release of information and you required to disclose to the Privacy Commissioner).
- University Executive.
- Senior Institutional Leaders.
- Board of Governors? (dependent on authority levels and governance structures)
- Broker/Insurer (if applicable).
- Law Enforcement.
- Students, Employees, Customers, etc. if there is an information breach.
- Media – proactive vs. reactive response.

Cybercriminals recruiting insiders to attack telecommunication providers: Kaspersky

Cybercriminals are using insiders to gain access to telecommunications networks and subscriber data, according to an intelligence report from global cybersecurity company Kaspersky Lab. In addition to targetting insiders, these criminals are also recruiting disillusioned employees through underground channels and blackmailing staff using compromising information... read more

Cyber attacks a growing problem for Canadian universities

Schools face a barrage of hacking attempts aimed in part at sensitive research

Nearly 70% of Canadian businesses hit by cyber attacks, says year-long survey

CTVNews.ca Staff
Published Wednesday, May 8, 2013 2:02PM EDT

Over a one-year period, 69 per cent of Canadian businesses said they experienced some type of cyber attack, ranging from malware and computer viruses to phishing and "social engineering" attacks, a new survey has found.

Canadian companies likely to pay ransomware demands, among highest for lost revenue and business interruption, international study finds

Companies in Canada are most likely to pay ransomware demands and are ranked among the highest for lost revenue and business interruption, according to an international study of 5,400 IT staff across Canada, the United States, the United Kingdom and... read more

UNIVERSITY OF CALGARY

The Attacks

Hackers breached the systems of health insurer Anthem, Inc., exposing nearly 80 million personal records.

Perhaps 2015's most high-profile hack was on Ashley Madison, the adultery website that promised its members discrete affairs.

An unknown group infiltrated hundreds of banks in multiple countries, swiping somewhere in the neighborhood of $1 billion.

Hackers gained access to unclassified White House systems in 2014, but the nature of the hack got way worse as new details emerged this year.

CIA Director John Brennan had his personal email hacked, which had sensitive personal documents in it.

Contact Us

QUESTIONS?

Janet Stein

Director, Risk Management & Insurance

Email: jstein@ucalgary.ca

Phone: 403-220-4623