Cyber Security in Higher Education: Why Universities are Prime Targets

Colin Couchman, Jeffrey Gardiner
With Special Guest Stephen Jarrett, Western University Legal Counsel

Thursday, February 23, 2017
Agenda

• Setting the Context and Breaking it Down
• PHISHing (and Spear PHISHing)
• High Profile Hacks
• Ransomware
• Why Are Higher Education Institutions Targets?
• Western University Information Technology Security Policy
  – “Why does this matter to you?”
• Discussion
The Context

- In the digital age, it is becoming easier and easier to get “lost” in all of the noise coming at us from multiple technology avenues.

- We need to be mindful of how information about us is being aggregated and used within countless contexts:
  - > 3.5 Billion Global Active Internet Users
  - > 2.5 Billion Social Media Accounts
  - > 4 Million Emails Per Second
  - > 200 Items Ordered on Amazon Per Second
  - > 3 million Google searches per minute
  - > 30 billion pieces of content added to Facebook per month
  - > 65 million tweets per day
  - 50 – 600 hours of content added to Youtube per minute
Breaking it Down

• What is a “Breach”?  
  – A data breach is the intentional or unintentional release of secure or confidential information to an untrusted entity.  
    • 40 percent increase from 2015  
    • This increase is despite regulatory scrutiny and more aggressive cyber-security spending  
    • Increased worldwide spending on security-related hardware, software and services rose to $73.7 billion in 2016 from $68.2 billion a year earlier, according to researcher; that number is expected to approach $90 billion in 2018  
    • Attacks known as phishing, in which an employee is tricked into clicking an e-mailed link to give hackers access to a corporate network, accounted for about 56 percent of all breaches last year  

(US data, Bloomberg)
PHISHing

- What is PHISHing?
  - the fraudulent practice of sending emails purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card number
PHISHing Example

We were unable to bill your membership for the current month. To ensure that the service will not be interrupted, please update your payment method.

To update your payment method, click: Sign In to Netflix then you will be prompted to update your payment method.
PHISHing Example

From: Western University <scvetko@uwo.ca>
Date: February 16, 2017 at 5:48:27 AM EST
To: [Redacted]
Subject: Official Email: Western Ontario Important Notifications

Dear,

Our record indicates that you recently made a request to terminate your Office365 email. And this process has begun by our administrator.

If this request was made accidentally and you have no knowledge of it, you are advised to cancel the

Please give us 24 hours !

Sign in here to cancel termination

Failure to cancel termination will result to closure of your account

Thanks
University of Western Ontario

Mailing Address

Office of Registrarial Services
Level 3, University Centre
Western University London,
Ontario, Canada,
N6A 3K7
PHISHing Example

From: Sarah
Sent: September-29-16 10:11 AM
Subject: Uwo.ca

Several of your incoming mails were placed on pending status due to a recent upgrade to our data. In order to receive the messages CLICKHERE to login and wait for response from Administrator, we apologize for any inconvenience and appreciate your understanding.

As always, your privacy and security are of utmost importance to us. We apologize if you have experienced any difficulties due to this situation, and please know that our technical staffs are working to solve the problem.

Regards,
Uwo.ca Technical Support team
PHISHing Example

In General:

Hello!
As part of our security measures, we regularly screen activity in the Facebook system. We recently contacted you after noticing an issue on your account: Our system detected unusual Copyrights activity linked to your Facebook account, please follow the links bellow to fill the Copyright Law form:

http://www.facebook.com/application_form

Note: If you don’t fill the application your account will be permanently blocked.

Regards,

Facebook Copyrights Department.
OTHER TYPES

• 2017 Tax Season Phish
• FedEx Shipment Update
• Important Announcement from President Chakma
• Irregular Activity with your Account
• Last Reminder You Must Update Your Apple Account Information!
• Google Docs Download
• "Dear Email User" Expired Password Ploy
Real World Impact

If Russia or any other country or person has Hillary Clinton's 33,000 illegally deleted emails, perhaps they should share them with the FBI!
Real World Impact

RUSSIAN HACKERS WERE FOUND IN THE DNC'S COMPUTER NETWORK.
Ransomware

- Defn: A type of malicious software designed to block access to a computer system until a sum of money is paid.

- Crypto-locked environment (storage, primary device)
- Nefarious actors request $ in return for crypto keys
- CNN Money reported $1B business in 2016 (by $500-$1000)
- ZDNet: 1 in 3 small businesses 'clueless' to the danger

- No need to spend time:
  - Identifying high value data
  - Exfiltration of Data
All your important files are encrypted.

At the moment, the cost of private key for decrypting your files is 2.5 BTC ~ $550 USD.

Your Bitcoin address for payment: [Address]

$ PURCHASE PRIVATE KEY WITH BITCOIN

You can also make a payment with PayPal My Cash Card

In case of payment with PayPal My Cash Card your total payment is $1000 USD (2 PayPal My Cash Cards)
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 MST

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 that point, we do have some encrypted machines. We have not used any of the decryption keys."
Cyber-Crime

Target
Announced: 12/13/2013
Though announced at the end of 2013, the effects of this breach carried into 2014. Target said its U.S. sales were "meaningfully weaker" after the data theft was disclosed.

Credit card numbers
Bank accounts
Social Security numbers
Proprietary information
Employee details
Email addresses
Physical addresses
Login credentials

110M

Stock dropped from $67/share - $61/share
46% drop in profits in Q4
+ 252M to reissue 21.8M credit cards
+100M to upgrade payment terminals to chip-n-pin
1-3M CC cards from this breach sold on black market
0 information security professionals employed before the breach
Cyber-Crime

Home Depot - Stock fell from $100/share - $88/share
$15.8 Billion loss in Market Capitalization
$3B in fake charges
+ 232M
- 100M insurance payout
Home Depot breach costs expected to reach billions

Owing to a slew of lawsuits filed by banks and credit unions, the expected cost to Home Depot for a cyber intrusion may reach into the billions, according to Insurance Business America (IBA).

The retailer recently stated it has already spent $232 million as a result of the breach last September, when hackers used a vendor’s stolen logon credentials to penetrate its computer network and insert malware that siphoned off payment-card data and email addresses of 56 million customers.

But that figure is projected to escalate as Home Depot contends with the
Cyber-Crime

Sony
Announced: 11/25/2014
Hackers broke into its network and exposed employment and salary records, documents and embarrassing private emails between Hollywood executives.

Sony Breach
Stock dropped from $22.15 to $20.78
$27.6 Billion lost in Market Capitalization
+ $35M first fiscal year
+ $252M to date
- $90M in insurance proceeds
Cyber-Crime

“The modern thief can steal more with a computer than with a gun. Tomorrow's terrorist maybe able to do more damage with a keyboard than with a bomb".

Question: Are Universities Prime Targets?

http://map.norsecorp.com/#/

So why do university's seem to have more than their fair share of cyber-attacks?

HINT: University’s aren’t prime targets.

Information IS!
So...Why Higher Education?

- Education is 3rd most targeted sector (Symantec) for breach attempts, behind Healthcare and Retail
- Higher Education is often distributed and decentralized
- Posture is typically “open”
- BYOD, non standardized equipment
- Cloud and Open Source
- Data-rich environment
  - Thousands of student records in each institution, with robust information
  - Research data
  - Patent data
  - Financial information
So...Why Higher Education?

• A large transient population
  – high volume of new personal, medical and financial data on hand
• Fresh data and profiles
  – large quantities of data each semester - hackers can steal large quantities of up-to-date data in a single attack.
• Plenty of time to do damage
• Numerous network and data access points
• High volume of network users
• Disparate silos of information and security
  – Separate units with autonomy and differing practices
### Viruses
Viruses infect computers through email attachments, file sharing and unpatched computers. They delete files, attack other computers, join botnets and otherwise make your computer run slowly. One infected computer can cause problems for all computers on a network.

### Hackers
Hackers are people who “trespass” into your computer from a remote location. They may use your computer to send spam or viruses, host a Web site, or do other activities that cause computer malfunctions. Social Engineering is associated with ‘Hackers’

### Identity Thieves
People who obtain unauthorized access to your personal information, such as Social Security and financial account numbers. They then use this information to commit crimes such as fraud or theft.

### Spyware / Botnets
Spyware is software that “piggybacks” on programs you download, gathers information about your online habits, and transmits personal information without your knowledge. It may also cause a wide range of other computer malfunctions.
Protecting the privacy and security of information and electronic resources at Western is an organizational priority. Technology is an integral component of all campus operations.

- The newly approved Computing, Technology & Information Resources policy (MAPP 1.13) outlines our collective responsibilities in safeguarding these critical resources.

- The responsibility for information security at Western is shared by every member of the campus community.

- Through positive information security behaviours we can all assist in protecting our valuable research, teaching and administrative information resources.

- The proper classification and handling of Western data throughout its lifecycle is critical element of this updated policy.
12 Principles

1. Overall responsibility for Security operations at the University lies with Information Technology Services (ITS), under the Associate Vice President of Institutional Budgeting, Planning & Information Technology (IT)
2. Academic Freedom is respected, but not to contravention of the Law
3. Everyone must abide by the University Code of Behaviour
4. Use of University systems and data should be limited to specific and authorized purposes
5. Individual users are responsible for the security and protection of any University data that they may need
6. Individual privacy rights must be respected and protected
7. Incidental personal & fair use of university systems is allowed, within reason
8. University provided Computing devices (including phones) and accounts are owned by Western
9. University supplied email addresses are designed as official for purposes of University communication
10. Protocols for handling University data will be informed by Western’s Data Classification standards
11. Specific provisions in negotiated Collective agreements may take precedence over the policy
12. Breaches of the policy will be arbitrated based on the user group(s) involved in the breach
Data Classification

- Understanding
- Creating
- Storing
- Archiving
- Destroying
- Sharing
- Using

#ProtectU
Raise your hand if you’ve read the fine print on every licensing agreement for software you’ve downloaded.

*Do these:*

Ensure that the university’s computing resources are used in an ethical and lawful manner.

Read and ensure you understand the Code of Behaviour as it applies to all users of the university’s computing resources.

*Don’t do these:*

Intentional use of computing resources for any purpose other than academic, administrative, and/or incidental, non-commercial personal use, will be considered to be unauthorized.

Use unlicensed or unauthorized copies of computer software.
Colin Couchman, Director, IMPACT Group, Faculty of Education, Western University
Jeffrey Gardiner, Central Information Security Officer (CISO), Western University
Stephen Jarrett, Legal Counsel, Western University