Cyber Security & Alberta Organizations

Presented by Jean Hernandez



Agenda

- 1. Cyber threat landscape
- 2. How to protect your organization
- 3. Where to learn more



Cyber threat landscape

Cybersecurity is often in the news.

The new reality: increased threats and increased scrutiny

• Grant McEwan University (2017)

- Defrauded \$11.8M in on-line phishing scam
- Equifax (2017)
 - Theft of personal data as a result of a software flaw
- WannaCry Attack (2017)
 - Encryption of data through ransomware attack on 200,000 outdated Microsoft-operated computers in 150 countries
- University of Calgary (2016)
 - Ransomware held staff email hostage until \$20,000 ransom was paid



Your identity is a steal on the Dark Web.

Here are what the most common pieces of information sell for



COLLEGE

Targeted attack motives

Known motives of targeted attack groups.

The majority of group are focused on intelligence gathering.

**Source; Symantec 2018 Internet Security Threat Report

Who are the victims?

24%

of breaches affected financial organizations.

15% 🔳

of breaches involved healthcare organizations.

12%

Public sector entities were the third most prevalent breach victim at 12%.

15%

Retail and Accommodation combined to account for 15% of breaches.

What tactics do they use?

62%

of breaches featured hacking.

51%

over half of breaches included malware.

81%

of hacking-related breaches leveraged either stolen and/or weak passwords.

43%

were social attacks.

14% I

Errors were causal events in 14% of breaches. The same proportion involved privilege misuse.

8%

Physical actions were present in 8% of breaches.

**Source: Verizon 2017 Data Breach Investigations Report

What else is common?

66% I

of malware was installed via malicious email attachments.

73% I

of breaches were financially motivated.

21%

of breaches were related to espionage.

27%

of breaches were discovered by third parties.

Does this happen at your organization?

- Someone uses the same **password** for all of their accounts
- Someone wants to **finish up a project at home** and sends confidential information to insecure home computer
- Someone takes a work laptop to use at a meeting at a Starbucks, using their unsecure wifi connection
- Someone checks their personal email on a company computer
- Someone clicks on a link in an email that looks like it came from their bank or a friend
- Your IT guy misses a virus protection installation on one of your company's computers

Who's your most dangerous offender?

What is phishing?

- Attempt (usually through email or other electronic communication like text) to obtain sensitive information such as usernames, passwords, and credit card details, often for malicious reasons, by disguising as a trustworthy entity.
- Phishing emails may contain links to websites that distribute malware.

Your Account | Queue | Help

Your Account Has Been Suspended

Dear Netflix,

We are sending this email to let you know that your credit card has been expired. To update your account information, please visit <u>Your Account</u>.

-Your friends at Netflix

Dear Tax Payer ,

You are entitled to your tax refund now. The tax refund amount is 651.44\$. You are required to follow the link below to login to our secure Epass site with your Social Insurance Number and complete the required information in order for your refund to be processed.

To access the form for your tax refund, please click here>>

Sincerely,

Canada Revenue Agency.

@Copyright Canada Revenue Agency. All rights reserved.

Hi <customer>,

This is a follow-up regarding your package delivery:

Tracking Number: <u>0p2uYq5RIho</u>

The package contained in the above-mentioned shipment was not accepted at the destination address. Please contact your local UPS office and provide the printed delivery sticker, included in this email.

Please note that in case of a failure to contact your local UPS office within 21 days the parcel will be returned to sender.

Thanks so much for shipping with UPS.

PayPal

We need your help

Your account has been suspended, as an error was detected in your informations. The reason for the error is not certain, but for security reasons, we have suspended your account temporarily

We need you to update your informations for further use of your PayPal account.

Update your information

You are currently made disabled of :

Adding a payment method Adding a billing address Sending payment Accepting payment

Please do not reply to this email. We are unable to respond to inquiries sent to this address. For immediate answers to your questions, visit our Help Center by clicking "Help" located on any PayPat page or email.

Copyright @ 2016 PayPal, Inc. All rights reserved. PayPal is located at 2211 N. First St., San Jose, CA 95131.

Refund Notification

Due to a sytem error you were double charged for your last order, A refund process was initiated but could not be completed due to errors in your billing information

REF CODE:2550CGE

You are required to provide us a valid billing address

Click Here to Update Your Address

After your information has been validated you should get your refund within 3 business days

We hope to see you again soon. Amazon.com Email ID:

	• 🐗 💷 🗸	0 01	A	122		
To:	ACCOUNTING DEPARTMENT					
Cc:	TomHeald@strategictax.com -					
Sub	oct: W2's for All Employees					
From	Tom Smith	Signature:	None		0	Tres ph
12						A 10-1

Please send our W2 Tax Documents for all employees to Tom Heald at Strategic Tax Consultants. I have cc'd him here.

We need these documents for a review ordered by the Board of Directors.

Please send immediately as we are under a time crunch.

Thanks,

Tom Smith CEO BetterSystems Inc

From: Sent: Tuesday, March 28, 2017 1:21 PM To: Subject: INSTRUCTION FOR WIRE TRANSFER

I need you to process a wire transfer to a new vendor. please let me know when you can get it done

Thanks

Hi

I want you to send me the list of W-2 copy of employees wage and tax statement for 2015, I need them in PDF file type, you can send it as an attachment. Kindly prepare the lists and email them to me asap.

....

Best way to avoid phishing

- Pause. Read. Think.
- Ask yourself:
 - Is this normal behavior?
 - Would I normally receive this type of message at this time of day?
 - Is this typical-sounding language from this individual?
- If in doubt, pick up the phone and call the sender instead.
- No professional organization will ever ask you to reveal personal or financial information over email or by going to a link.

What is malware?

• Short for "malicious software"

- Umbrella term that includes:
 - Viruses
 - Ransomware
 - Spyware
 - And others

Rapidly growing cyber black market

Cyber Black Market

Bitcoin

Who is behind the breaches?

75%

perpetrated by outsiders.

25%

involved internal actors.

18% I

conducted by state-affiliated actors.

3% featured multiple parties.

2%

involved partners.

51%

involved organized criminal groups.

**Source: Verizon 2017 Data Breach Investigations Report

Typical attack life cycle

Cyber security program

Protect what matters the most

Being attacked is unavoidable, so how prepared are you? Can you answer "yes" to these five key questions?

Embed cybersecurity into every role to protect your most critical assets

Where to start

• Identify your assets enabling critical business processes

• Identify your sensitive data

• Establish a security controls baseline

- Malware protection software on computers and servers
- Regular patch management practices (infrastructure and applications)
- Network security controls (internet access and e-mail protection)
- Identity and access management controls
- Regular back-ups and recovery testing

Threat detection and response

- Define, implement and sustain a cyber incident response process
- Define, implement and sustain security monitoring capabilities
- Define, implement and sustain vulnerability identification and risk mitigation processes

Key attributes of an Incident response plan

Want to learn more?

- Canadian Cyber Incident Response Centre (CCIRC)
 - <u>https://www.publicsafety.gc.ca/cnt/ntnl-scrt/cbr-scrt/ccirc-ccric-en.aspx</u>
- Center for Internet Security (CIS)
 - https://www.cisecurity.org/controls/
- National Institute of Standards and Technology (NIST)
 - https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

Employee training options

InnoTech College:

- (ISC)2 Certifications
 - Certified Information Systems Security Professional (for operational leaders)
 - Systems Security Certified Practitioner (for IT professionals)
- Arcitura Certifications
 - Cloud Architect
 - Cloud Security

Other Educational Institutions:

- SAIT IT Security Certificate
- NAIT System Security Certificate

Questions?

Jean Hernandez Cyber Security Consultant InnoTech College jeanh@innotechcollege.com

