



# 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

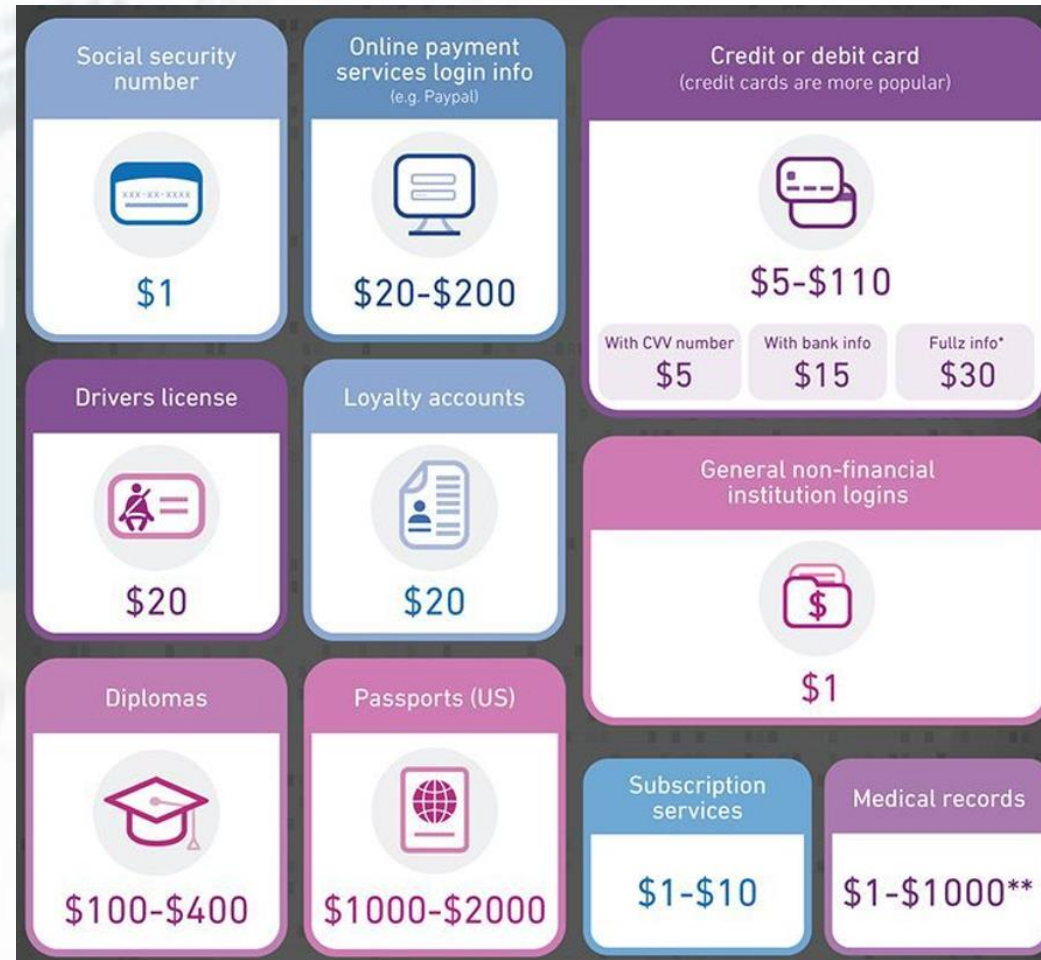
Cybersecurity is often in the news.

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  - Encryption of data through ransomware attack on 200,000 outdated Microsoft-operated computers in 150 countries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

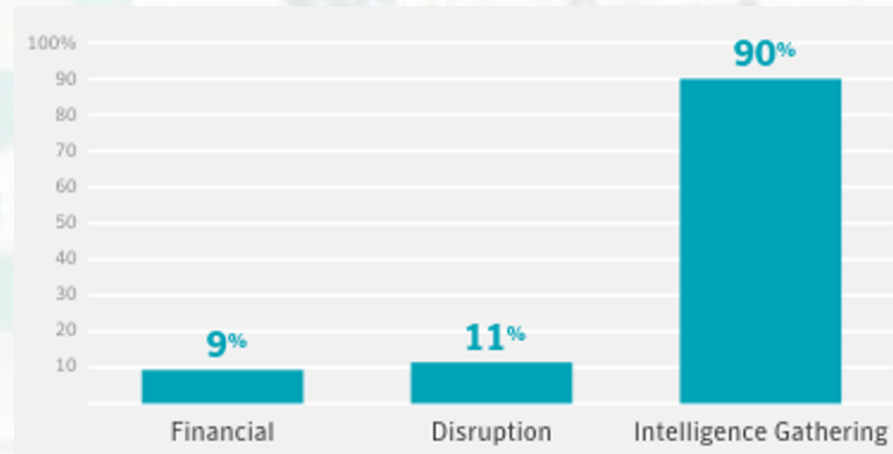
# Your identity is a steal on the Dark Web.

Here are what the most common pieces of information sell for

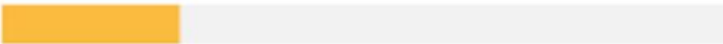


# Targeted attack motives

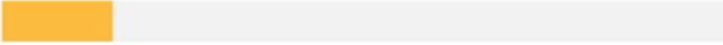
Known motives of targeted attack groups.  
The majority of group are focused on intelligence gathering.



# Who are the victims?

**24%** 

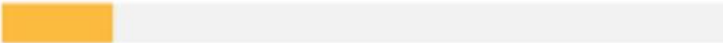
of breaches affected financial organizations.

**15%** 

of breaches involved healthcare organizations.

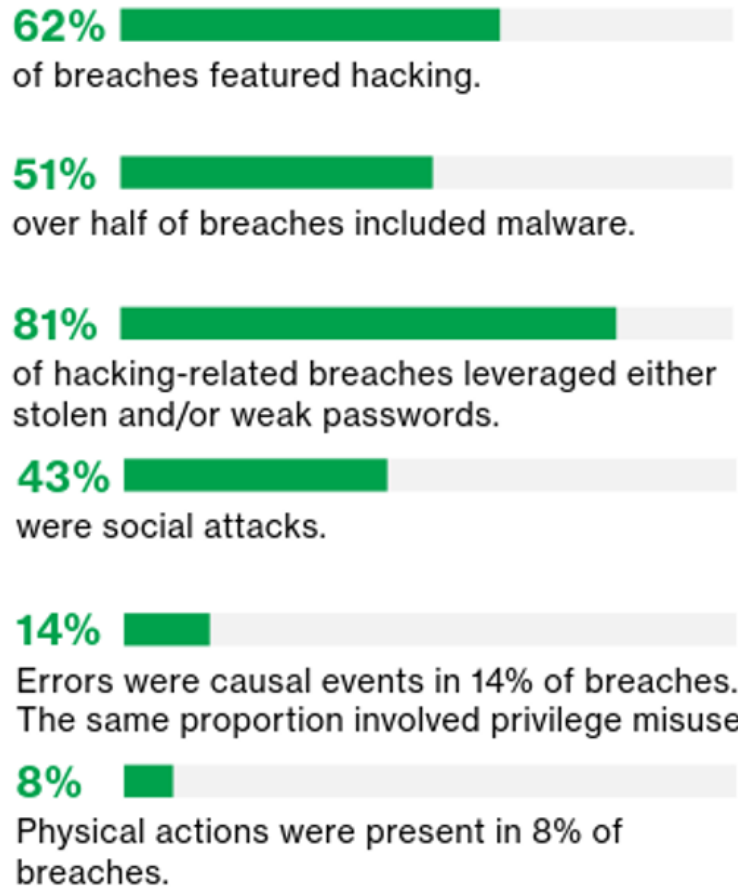
**12%** 

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

**15%** 

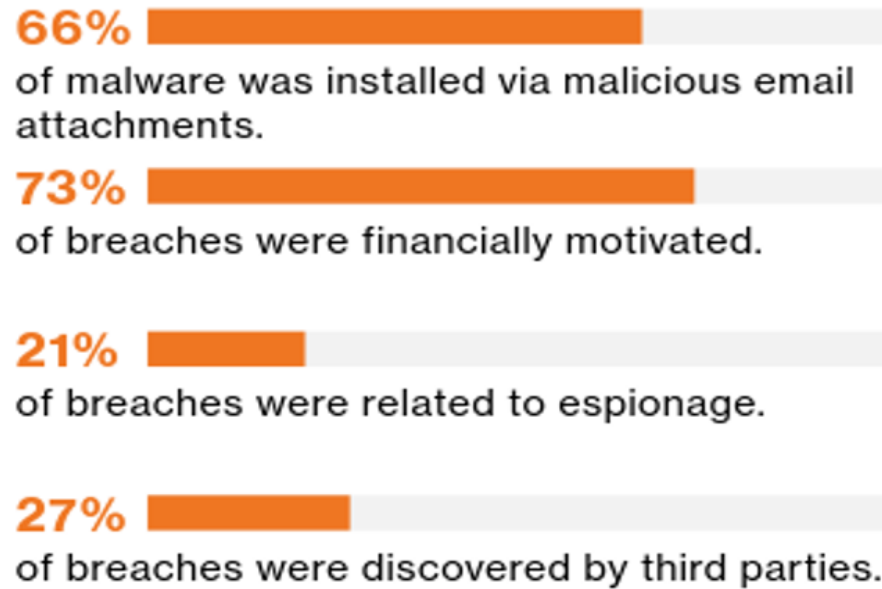
Retail and Accommodation combined to account for 15% of breaches.

# What tactics do they use?





# What else is common?





# 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**.

# Sample phishing email

**NETFLIX**

[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 [Your Account](#).

-Your friends at Netflix

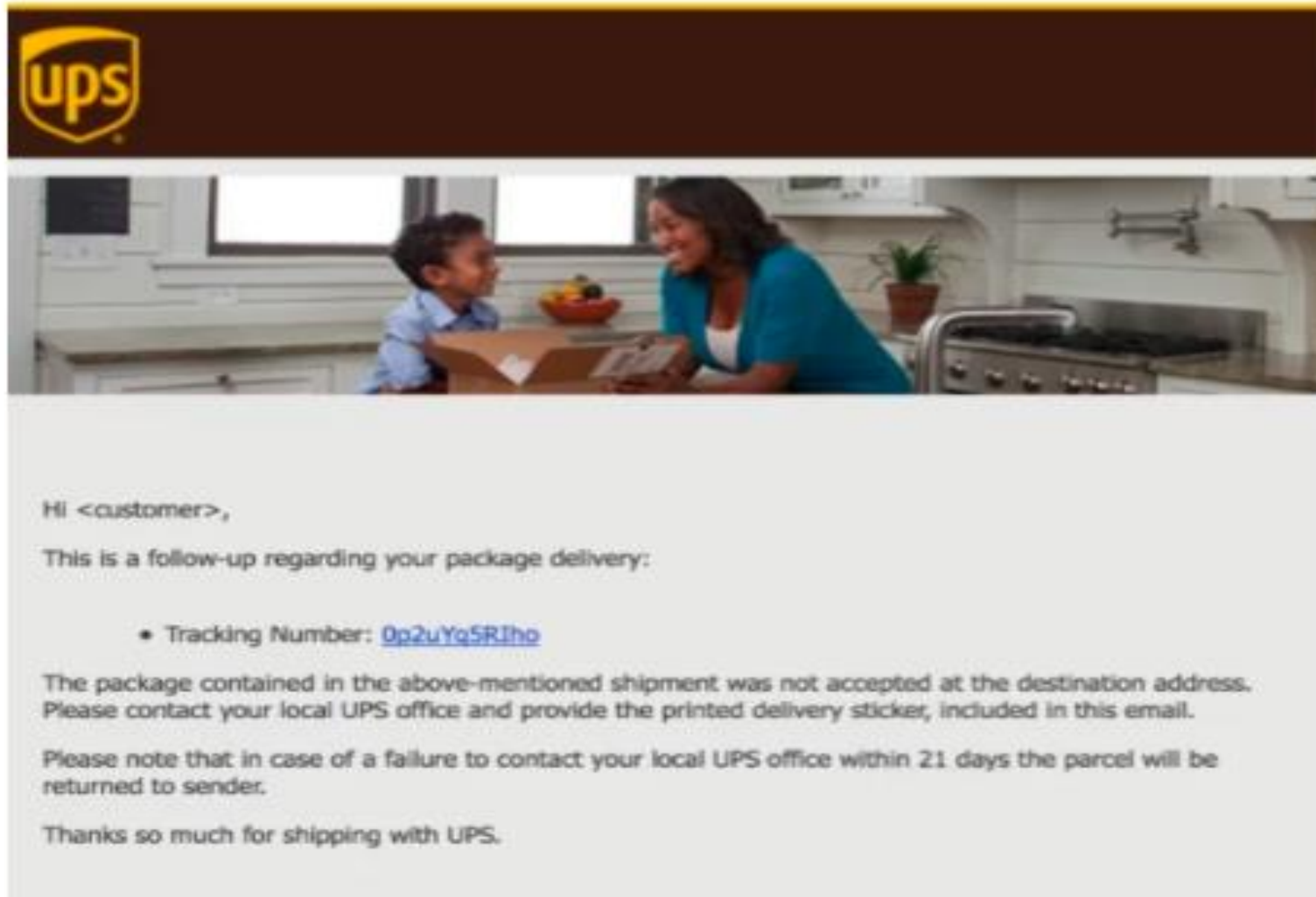
# Sample phishing email



©Copyright Canada Revenue Agency. All rights reserved.



# Sample phishing email



# Sample phishing email



# 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 PayPal page or email.

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



# Sample phishing email



## Refund Notification

Due to a system 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](#)

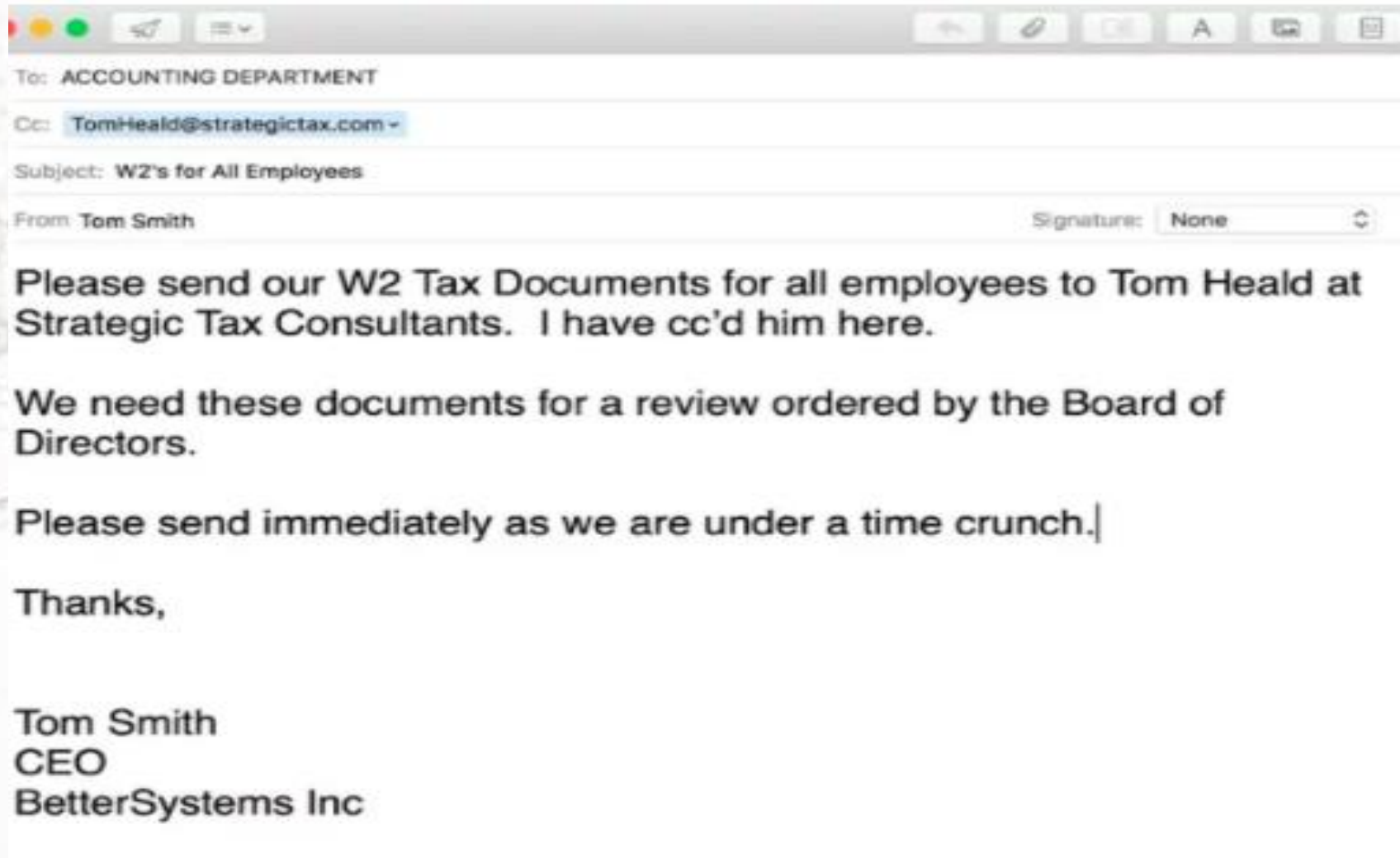
After your information has been validated you should get your refund within 3 business days

We hope to see you again soon.

[Amazon.com](#)

Email ID: [REDACTED]

# Sample phishing email



# Sample phishing email

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

Hi [REDACTED]

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

Thanks  
[REDACTED]

# Sample phishing email

Urgent Request

Inbox x



Mr. [Redacted]

7:50 AM (1 hour ago)



to me

Alanna

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

Dark Web/Dark  
Net/Deep Web



Cyber Black  
Market

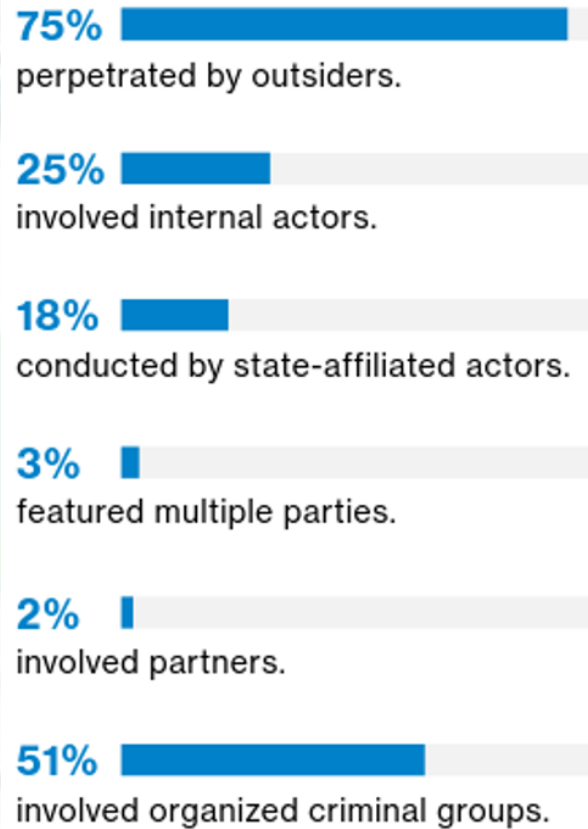


Bitcoin

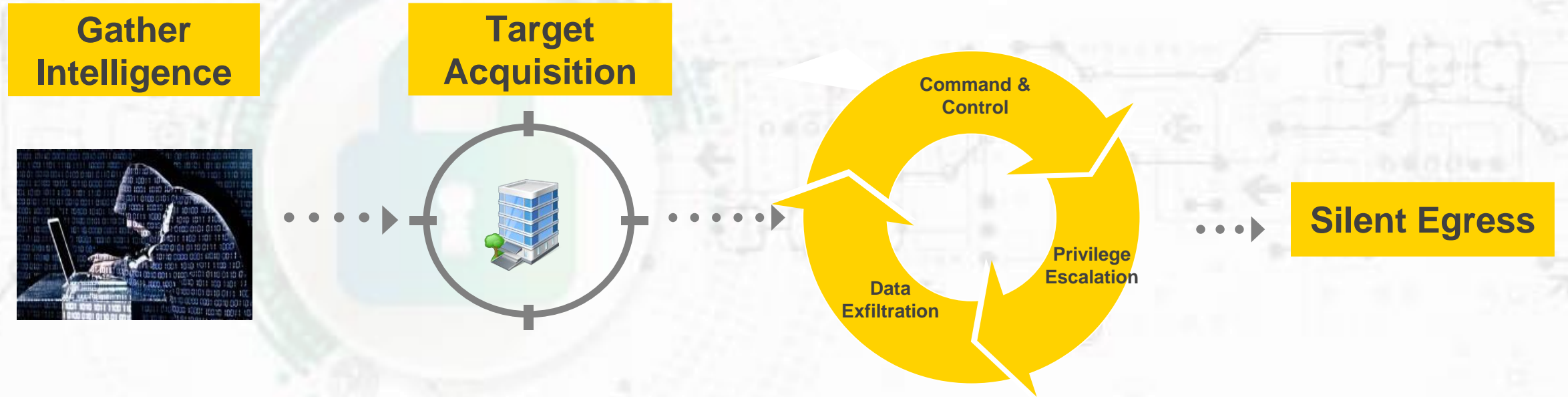




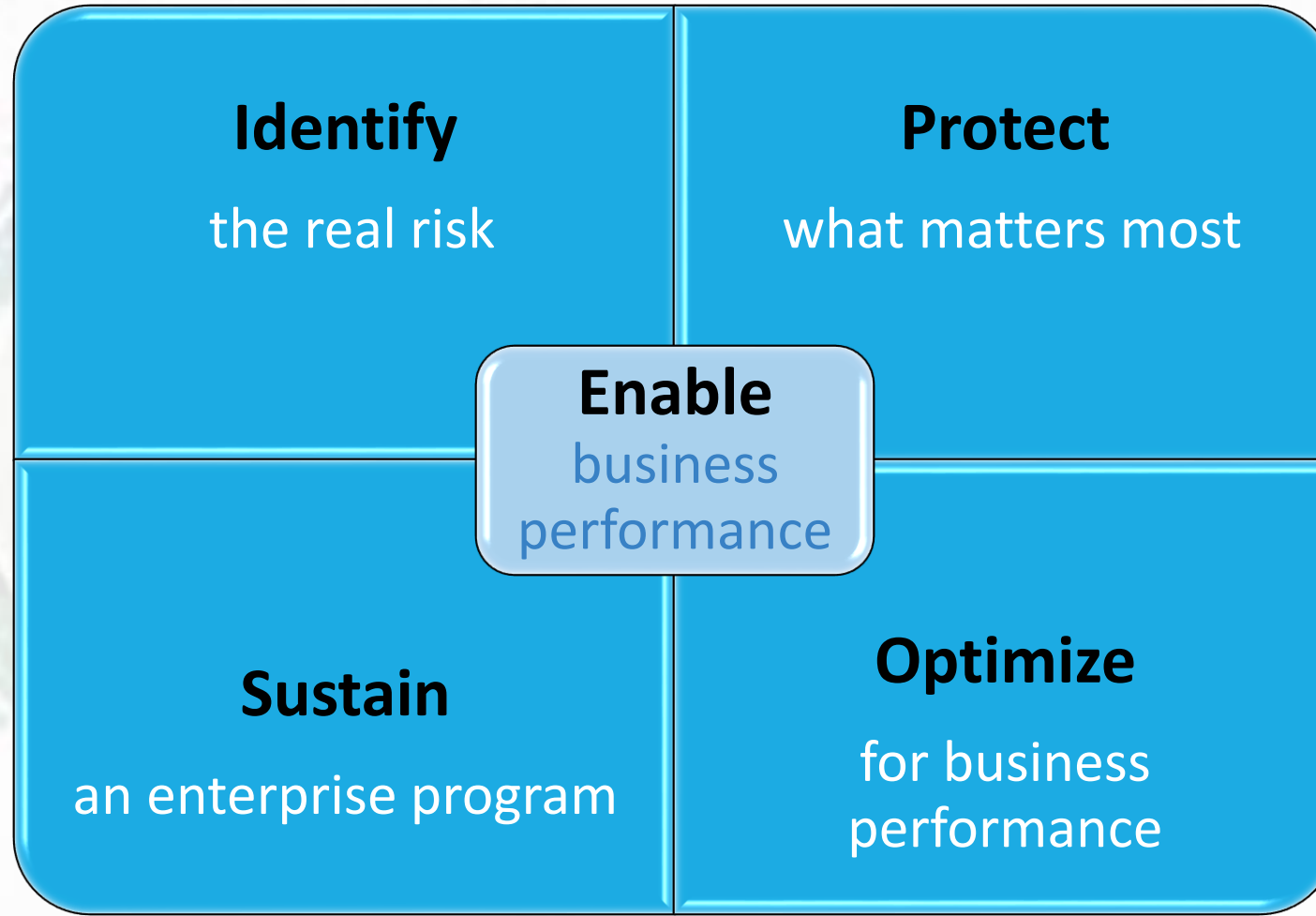
# Who is behind the breaches?



# Typical attack life cycle

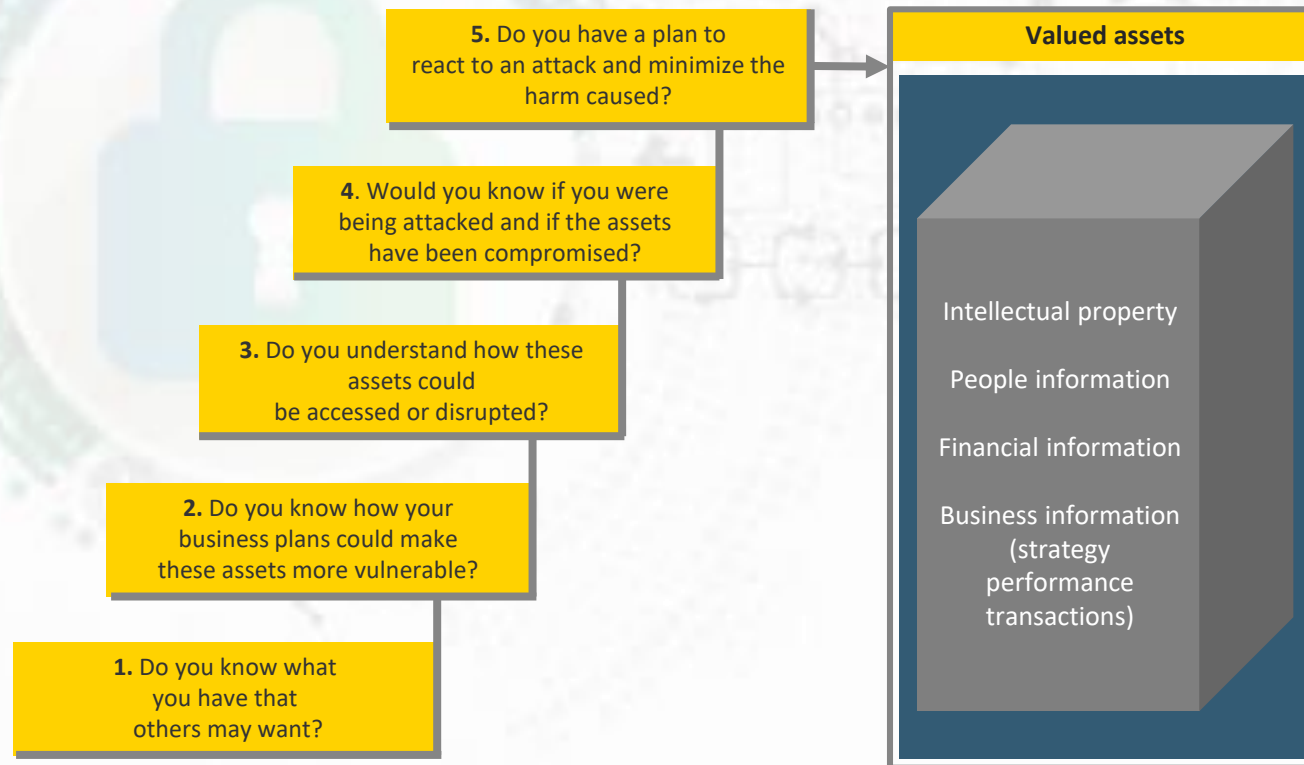


# Cyber security program

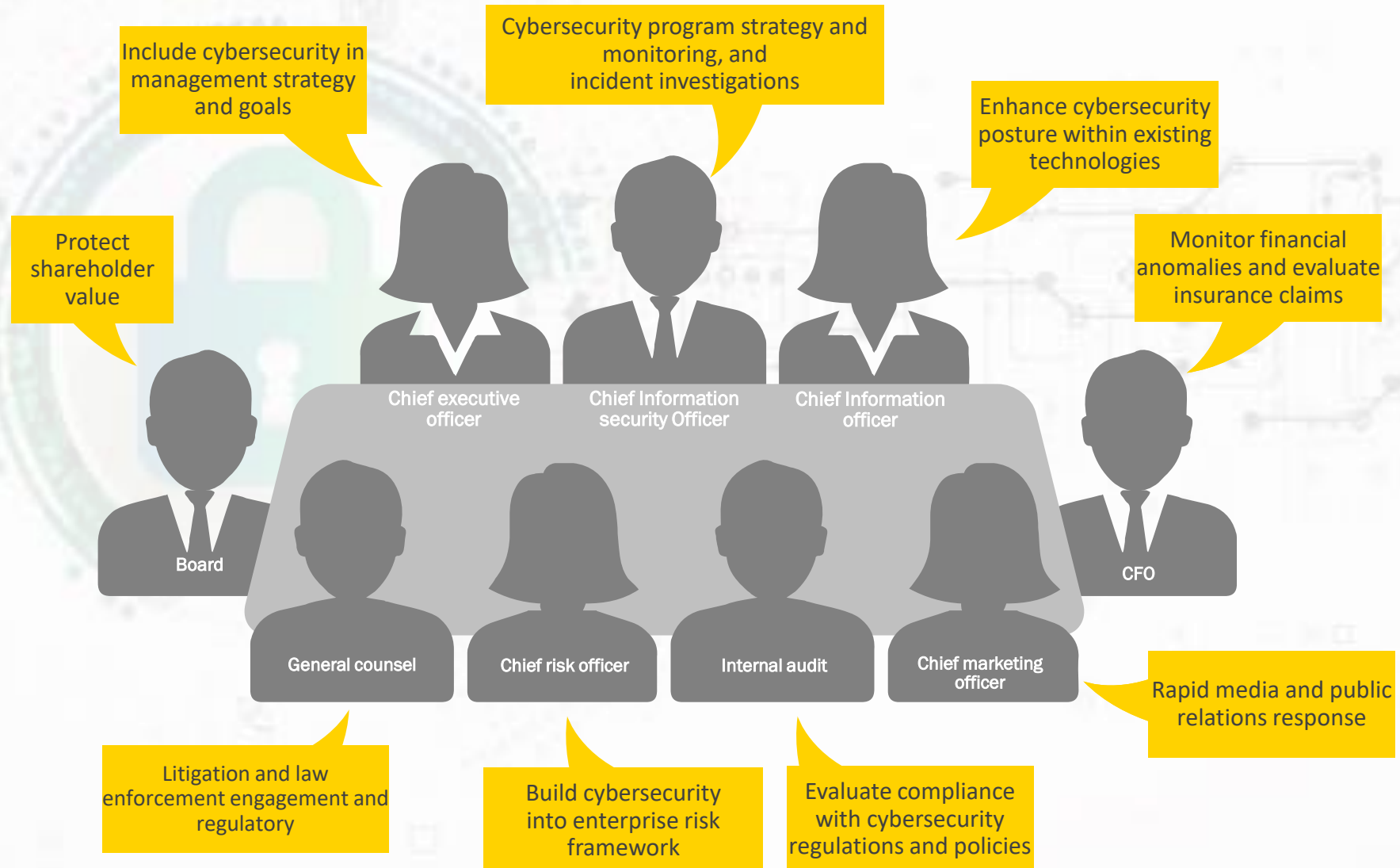


# Protect what matters the most

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)
  - <https://www.publicsafety.gc.ca/cnt/ntnl-scr/cbr-scr/ccirc-ccric-en.aspx>
- 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](mailto:jeanh@innotechcollege.com)