Cyber Security Webinar

FSRA

Financial Services Regulatory Authority of Ontario

Date: November 29, 2022

VT INCEPIT FIDELIS SIC PERMANET

Ontario

Our Presenters

Caroline Blouin
FSRA
Executive Vice-President,
Pensions

David Bartucci
FSRA
Head, Pensions Stakeholder
Relations and Special Projects

Ted Harman
Accent Insurance Solutions
President

Ryan Wilson
EY Canada
Cybersercurity Partner

Agenda

- Introductions and Ground Rules
- Hearing from the Experts – Ted Harman Shares his Experience
- Taking the Pulse of Ontario’s Pension Sector – Key Survey Findings
- Regulatory Approach – Highlights of New CAPSA Guidance
- Hearing from the Experts – Ryan Wilson Shares Information on Understanding Threats, Why this is Important and What Administrators Should Think About

FSRA

Financial Services Regulatory
Authority of Ontario

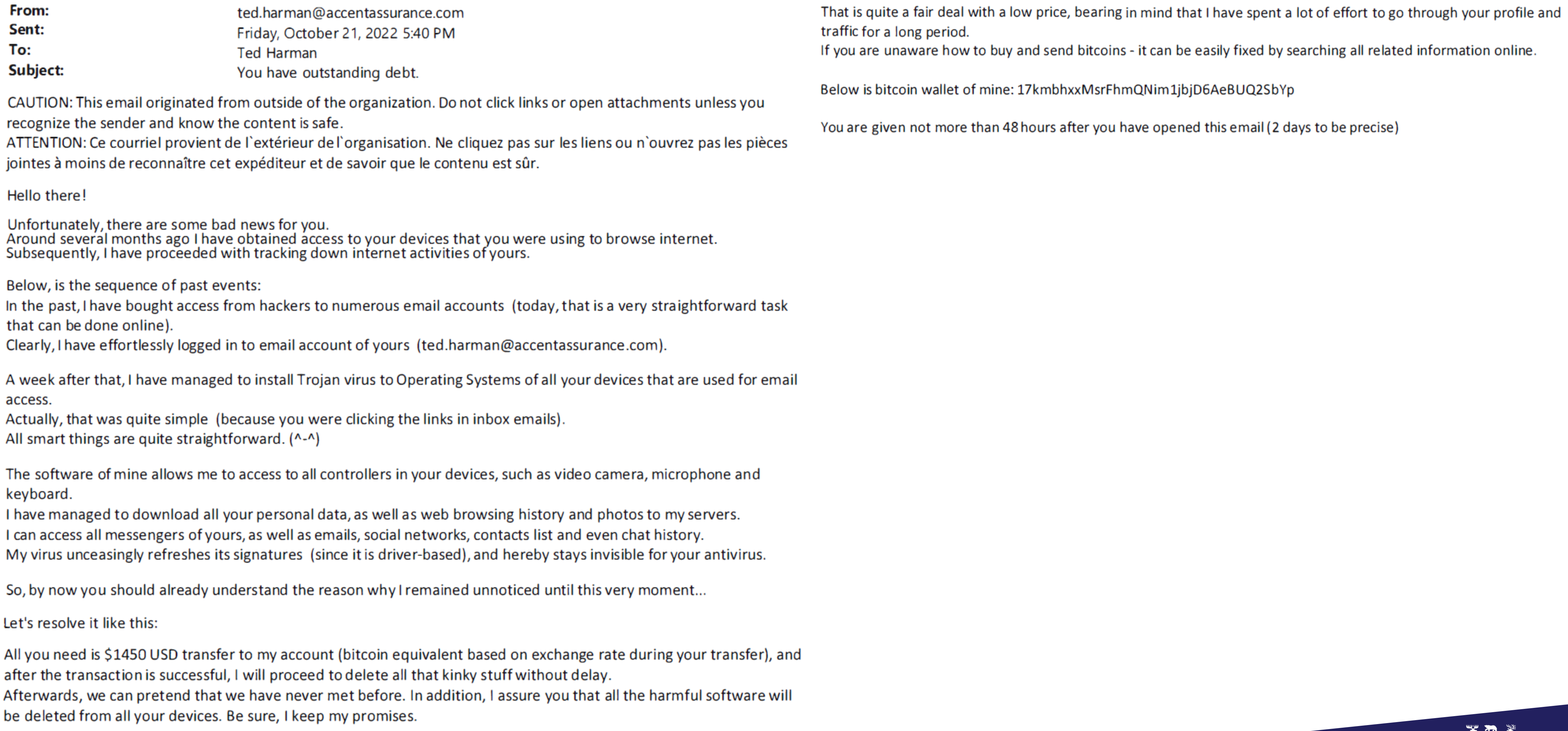
Ontario

Hearing from the Experts – Ted Harman Shares his Experience

- Future Electronics v. Chubb
- Personal cyber extortion threat
- Resources

FSRA
Financial Services Regulatory Authority of Ontario

Hearing from the Experts – Ted Harman’s Extortion Attempt



From: ted.harman@accentassurance.com
Sent: Friday, October 21, 2022 5:40 PM
To: Ted Harman
Subject: You have outstanding debt.

CAUTION: This email originated from outside of the organization. Do not click links or open attachments unless you recognize the sender and know the content is safe.
ATTENTION: Ce courriel provient de l`extérieur de l`organisation. Ne cliquez pas sur les liens ou n`ouvrez pas les pièces jointes à moins de reconnaître cet expéditeur et de savoir que le contenu est sûr.

Hello there!

Unfortunately, there are some bad news for you.
Around several months ago I have obtained access to your devices that you were using to browse internet.
Subsequently, I have proceeded with tracking down internet activities of yours.

Below, is the sequence of past events:
In the past, I have bought access from hackers to numerous email accounts (today, that is a very straightforward task that can be done online).
Clearly, I have effortlessly logged in to email account of yours (ted.harman@accentassurance.com).

A week after that, I have managed to install Trojan virus to Operating Systems of all your devices that are used for email access.
Actually, that was quite simple (because you were clicking the links in inbox emails).
All smart things are quite straightforward. (^-^)

The software of mine allows me to access to all controllers in your devices, such as video camera, microphone and keyboard.
I have managed to download all your personal data, as well as web browsing history and photos to my servers.
I can access all messengers of yours, as well as emails, social networks, contacts list and even chat history.
My virus unceasingly refreshes its signatures (since it is driver-based), and hereby stays invisible for your antivirus.

So, by now you should already understand the reason why I remained unnoticed until this very moment...

Let's resolve it like this:

All you need is $1450 USD transfer to my account (bitcoin equivalent based on exchange rate during your transfer), and after the transaction is successful, I will proceed to delete all that kinky stuff without delay.
Afterwards, we can pretend that we have never met before. In addition, I assure you that all the harmful software will be deleted from all your devices. Be sure, I keep my promises.

That is quite a fair deal with a low price, bearing in mind that I have spent a lot of effort to go through your profile and traffic for a long period.
If you are unaware how to buy and send bitcoins - it can be easily fixed by searching all related information online.

Below is bitcoin wallet of mine: 17kmbhxxMsrFhmQNim1jbjD6AeBUQ2SbYp

You are given not more than 48 hours after you have opened this email (2 days to be precise)

Taking the Pulse – Key Findings from FSRA's First Cyber Security Survey

Financial Services Regulatory Authority of Ontario

20

SURVEY RESPONSES

Survey sent randomly to plans of varying size and across the sector:

- **DB plans**
- **MEPPs**
- **DC**

1. Cybersecurity Controls

- Cybersecurity team varied from 1 – 349 number of resources
- **Policy**: Almost all have a policy in place, about half reviewed annually; small number had no explicit policy in place

Endpoint Security Controls*	Yes
Advanced malware protection (including zero-day protection)	17
Data Loss Prevention (DLP) technology	10
Endpoint Detection and Response (EDR)	13
Full disk encryption	12
Industry recognized system hardening standard(s) (e.g., CIS)	8 (1 in progress)
Traditional antivirus / malware protection	18

*1 responder removed from the count

2. Third Parties

- **TPRM:** Just under half have TRPM in place, with most TRPM program integrated with vendor management
- **Results**: Most responders with third-party providers have a formalized regulatory, legal and compliance program in which they share their results or attestation of compliance

Taking the Pulse – Key Findings from FSRA's First Cyber Security Survey

3. Incident Reporting

❑ **Incident Response Plan and Policy:** Most have a policy, 1 in progress, a few have none

❑ **Post Incident Activities:** All perform incident activities

4. Risk Exposure

❑ **Risk Assessments**: More than half adopted standard methodology to perform cyber and privacy risk assessments. Just over half perform formalized cyber risk assessments

❑ **Information Data:** All are collecting and storing any personally identifiable information. More than half are collecting protected health or medical information

5. Human Controls

❑ **Training Program:**

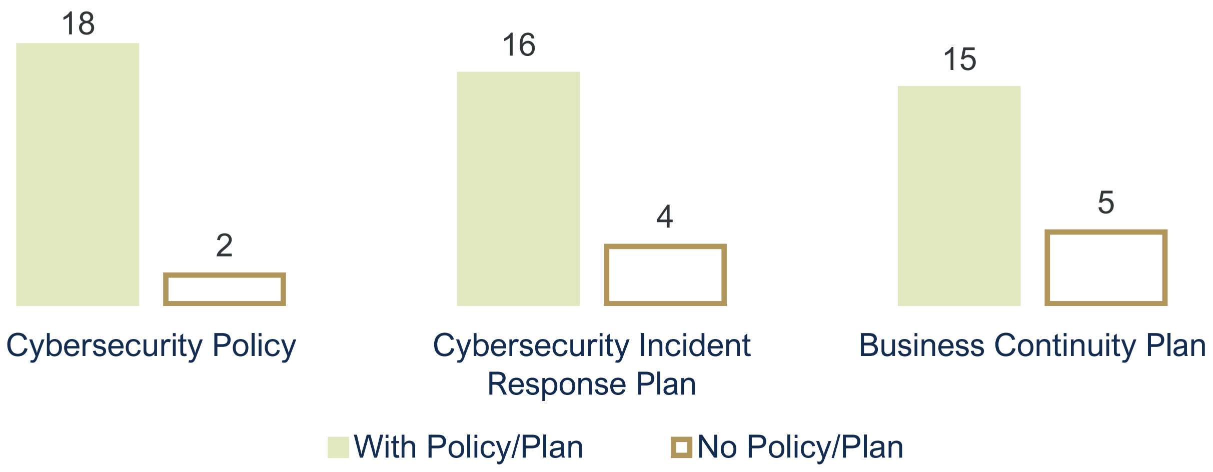
  ❑ Most have a formalized security awareness training program

  ❑ Just under half have specialized cyber risk related training on how to safely administer funds

❑ **Testing**: Nearly all perform ongoing phishing and user susceptibility testing

Taking the Pulse – Key Findings from FSRA's First Cyber Security Survey

- ❑ Most plans have a Cybersecurity Policy in place. Given the relatively small size of the sample, it's hard to draw an average team size of cybersecurity professionals. Some organizations have as few as 1 cybersecurity professional.



- ❑ Regulatory, legal and compliance obligations related to cybersecurity, data protection and privacy varied and can include one or more the following: OSFI, AMF, PCI, DSS, PIPEDA, GDPR, OSFI.
  - ❑ 15 answered yes to reporting cyber breaches to regulatory and required authorities; 5 answered no.

Taking the Pulse – Key Findings from FSRA’s First Cyber Security Survey

- 100% have in place the ability to monitor all IT systems (inclusive of outsourcing agreements for any systems and applications) against cyber-attacks.
  - Some plans report only monitoring during business hours

- 100% perform post-incident activities to validate an incident has been resolved adequately following a breach or security incident.

- The types most common to successful cybersecurity attacks that organizations experienced over the past 12 months:

1. Phishing
2. Credential Compromise
3. Denial of Service Attacks
4. Ransomware

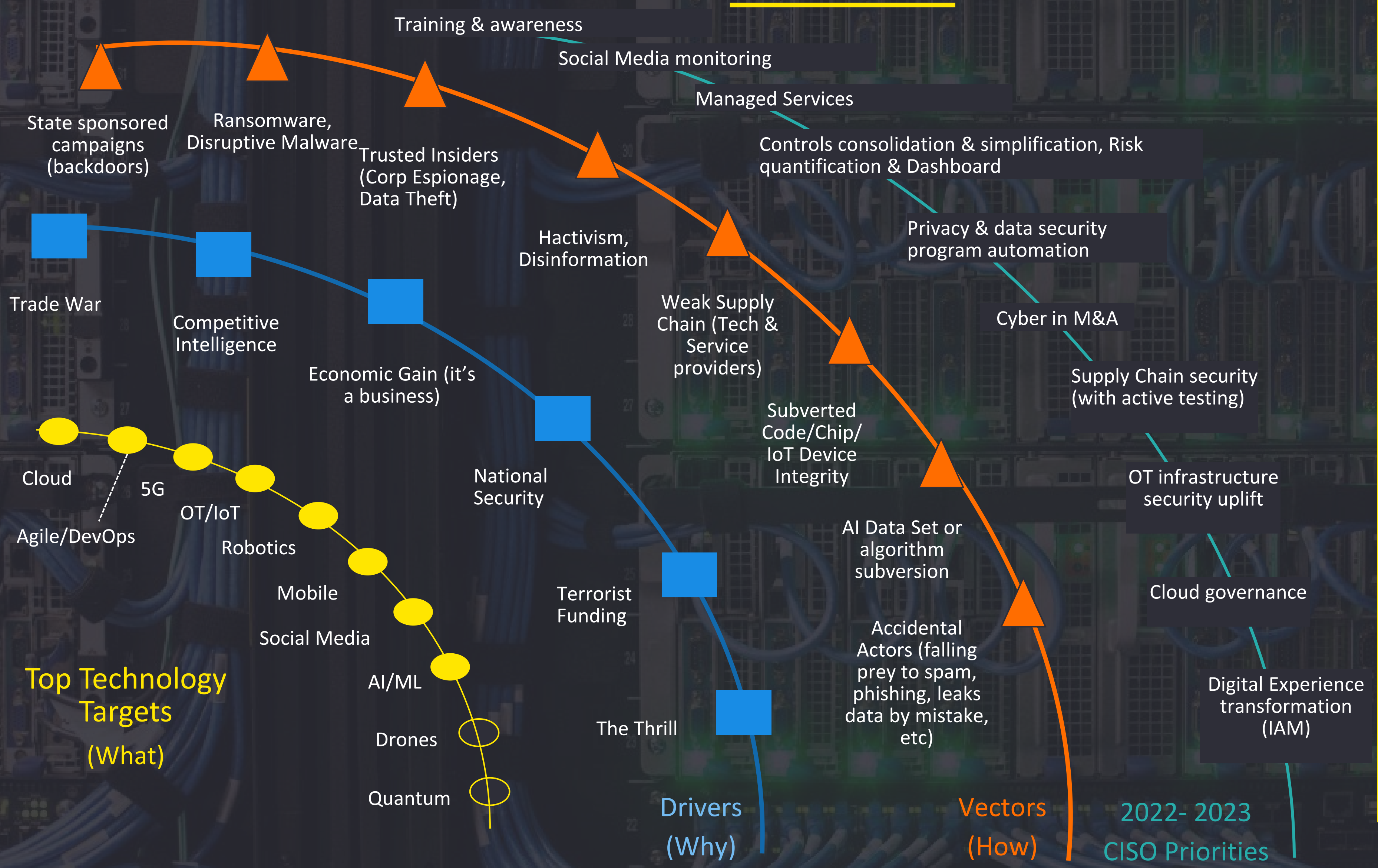
Regulatory Approach

- FSRA is a member of the Canadian Association of Pension Supervisory Authorities (CAPSA). CAPSA has prioritized both risk management and cyber security.
- CAPSA published a draft cybersecurity guideline for public comment in June – comments are being reviewed now. CAPSA also received supportive feedback on integrating it into broader risk management guideline.
- New Risk Management Guideline, including a section dedicated to cyber security is being developed now, with the aim of public consultation in spring 2023.
- The draft Cyber Security Guideline is available on CAPSA's website - capsa-acor.org

Key Concepts from the Draft Guideline

- Cyber risk is a key risk for all plans, regardless of plan size or characteristics. It should be regularly reviewed and assessed to ensure appropriate controls are in place to allow the plan to manage the risk. Cyber risks are complex and evolving and require a dynamic response.
- In discharging their fiduciary responsibilities, plan administrators should ensure that the plan has access to the required skills, expertise and/or training to understand and manage cyber risk.
- Roles and responsibilities relating to cyber risk should be clearly defined, assigned, and understood, including with respect to any activities delegated to third-party service providers (and all applicable subcontractors).
- Plan administrators should have a strategy in place for responding to and reporting cyber incidents.

Understanding the Cyber Threat, Methods and Motives



Top Technology Targets

(What)

Cloud

5G

Agile/DevOps

OT/IoT

Robotics

Mobile

Social Media

AI/ML

Drones

Quantum

Drivers

(Why)

Trade War

Competitive Intelligence

Economic Gain (it's a business)

National Security

Terrorist Funding

The Thrill

Vectors

(How)

State sponsored campaigns (backdoors)

Ransomware, Disruptive Malware

Trusted Insiders (Corp Espionage, Data Theft)

Hactivism, Disinformation

Weak Supply Chain (Tech & Service providers)

Subverted Code/Chip/ IoT Device Integrity

AI Data Set or algorithm subversion

Accidental Actors (falling prey to spam, phishing, leaks data by mistake, etc)

2022- 2023

CISO Priorities

Training & awareness

Social Media monitoring

Managed Services

Controls consolidation & simplification, Risk quantification & Dashboard

Privacy & data security program automation

Cyber in M&A

Supply Chain security (with active testing)

OT infrastructure security uplift

Cloud governance

Digital Experience transformation (IAM)

Takeaway: Disclosures suggest cyber attacks are largely focused on financial gain, contributing to two major themes: ransomware and the theft of intellectual proprietary or personal information.

Also, attacks which focus on shutting down key systems within an organization can still lead to financial loss even if customer data is not exfiltrated.

Cyber risks exists across all organizations, regardless of size.

What is Cybersecurity and why is it important to you?

Cyber risk can be understood within the following ….

Risk = threat x vulnerability x impact

threat: (prevalence of the threat)

vulnerability: (likelihood vulnerability can be exploited)

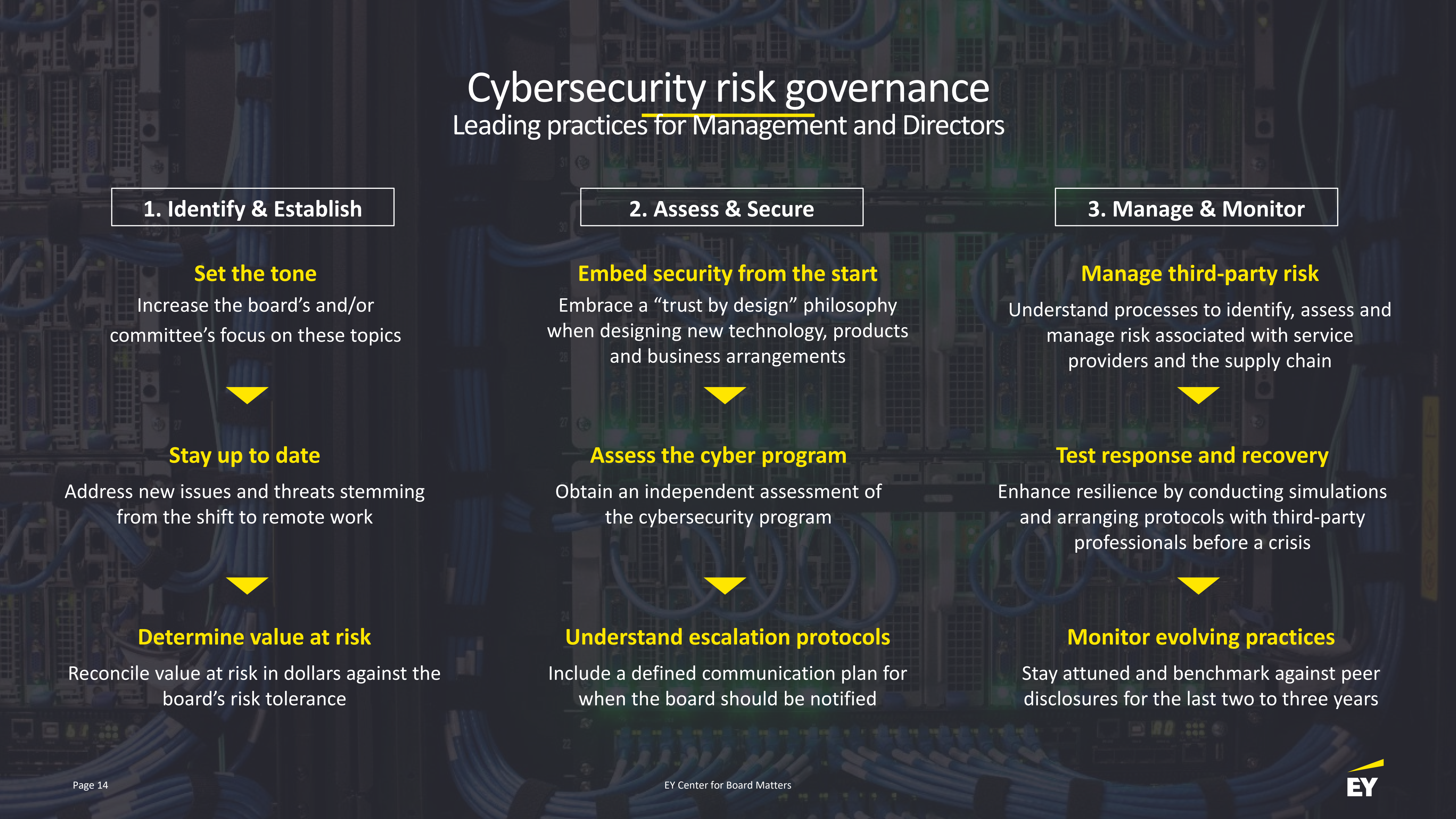
impact: (the potential financial, operational, legal or regulatory effect)

- **Cyber threats are stealthier, more sophisticated**
  - More than 200K threats are released into the wild each day, only 56% of threats are "detectable"
  - Insiders unwittingly enable 95% of attacks
  - Hacktivists are now second largest attack group
- **Number of vulnerabilities (attack surface) is increasing**
  - Covid drove 10 years of innovation in <1 year
  - Interconnectivity with third parties
- **Form of impact is also changing**
  - Total percentage of disruptive attacks (ex. ransomware) has risen 59% between 2020 and 2021
  - Cybersecurity is becoming an increasingly prevalent ESG/Sustainability topic

Recent Headlines

- ► Pension Plan Personal Data Breached, Third-Party Blamed
- ► Pension plan loses $3.5M after cyber attack
- ► Data breach affects pension provider, 50,000 victims
- ► Pension plan (401k) triggers suit against plan fiduciaries

Takeaway: The size and complexity of cyber attacks is increasing rapidly.



Cybersecurity risk governance

Leading practices for Management and Directors

1. Identify & Establish

Set the tone

Increase the board's and/or committee's focus on these topics

Stay up to date

Address new issues and threats stemming from the shift to remote work

Determine value at risk

Reconcile value at risk in dollars against the board's risk tolerance

2. Assess & Secure

Embed security from the start

Embrace a "trust by design" philosophy when designing new technology, products and business arrangements

Assess the cyber program

Obtain an independent assessment of the cybersecurity program

Understand escalation protocols

Include a defined communication plan for when the board should be notified

3. Manage & Monitor

Manage third-party risk

Understand processes to identify, assess and manage risk associated with service providers and the supply chain

Test response and recovery

Enhance resilience by conducting simulations and arranging protocols with third-party professionals before a crisis

Monitor evolving practices

Stay attuned and benchmark against peer disclosures for the last two to three years

Questions

Closing Remarks

Thank you for attending.

Additional questions following the webinar may be sent to Karima.Shajani@fsrao.ca