IMPLICATIONS OF A CYBER BREACH

Building your response plan(s)

HELLO

MY NAME IS

Garth

AGENDA

- Background
  - Discussion of cybersec history and types of cyber events
- Implications
  - Impacts to consider when planning
- Integrating Cyber Response into BC
  - Group exercise

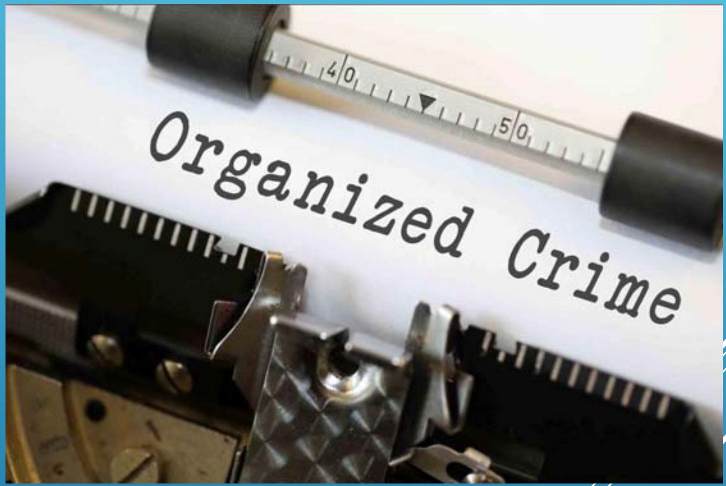
BACKGROUND

Origins/Causes of Cyber Crime

- Organized crime
- State sponsored espionage
- Terrorist groups

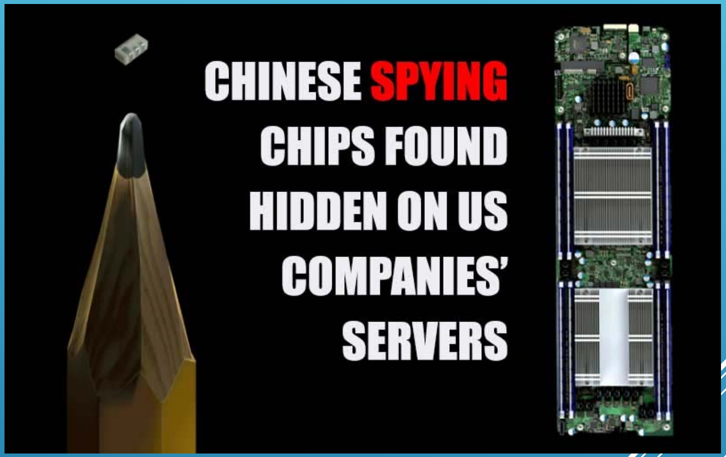
ORGANIZED CRIME

- Many OC groups have a specialization in cyber crime, both foreign and domestic
- Types of cyber crime
  - Phishing
  - Ransomware
  - DDoS
  - Viruses
  - Malware
  - Spoofing
  - Social engineering
  - Identity theft
  - Etc…



STATE SPONSORED

- Foreign governments aren't looking for a payout as OC would, they're looking for secrets or competitive advantage in trade or manufacturing
  - Espionage
    - Industrial
    - Military
  - Election interference
  - Critical Infrastructure Attacks



TERRORIST GROUPS

- They thrive on chaos in the targets of their hacking campaigns as well as attacking infrastructure (telecoms, utilities, etc.)

IMPLICATIONS

Effects of a cyber breach

- Reputational Harm
- Legal / Breaches of Contract
- Financial Loss
- Social and Psychological Effects
- Operational Disruption

REPUTATIONAL HARM

- Is this listed in your corporate risk register?

And

- Has your DRI Certified BC Professional assessed it using DRI PP #2

If Yes

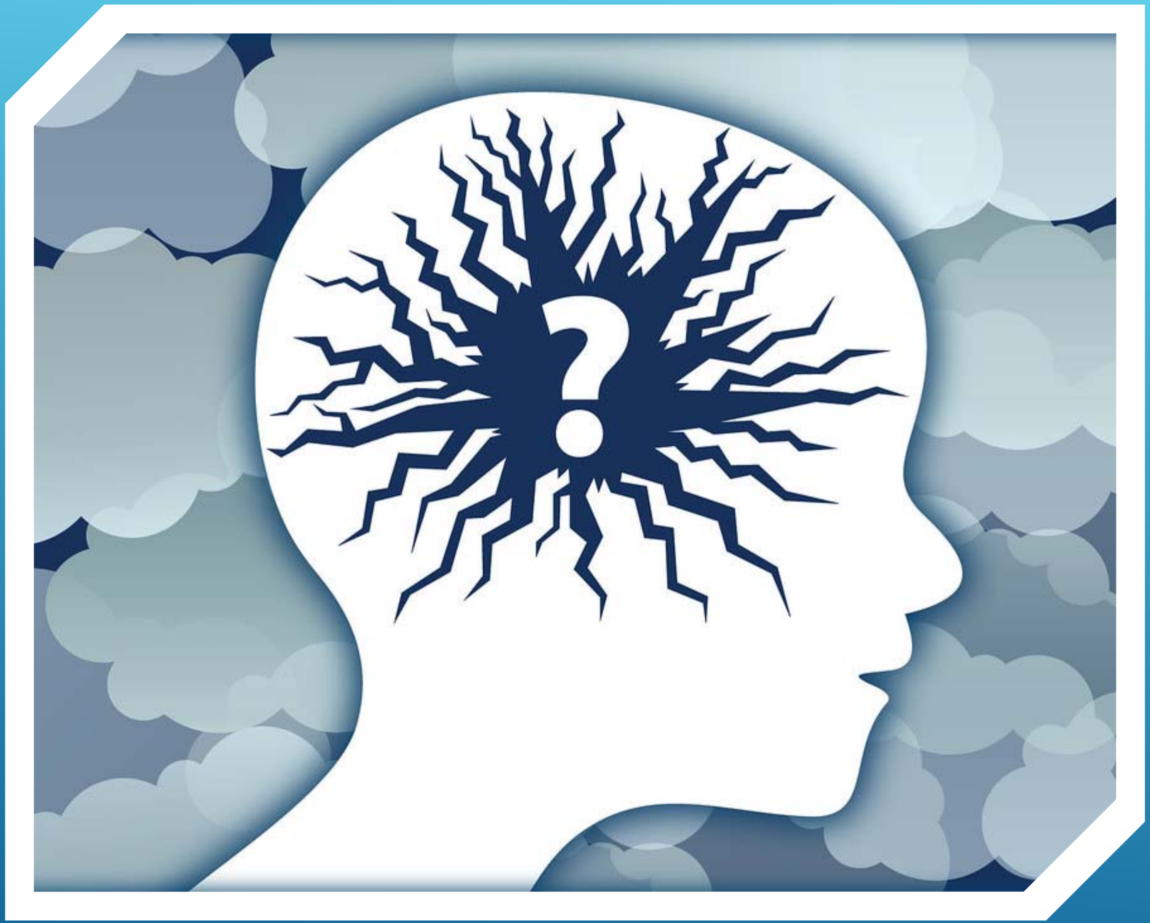
- Then the business leaders must determine how much they are willing to invest in protecting the business

LEGAL / BREACHES OF CONTRACT

- Canadian courts have upheld that cyber penetration is a breach of contract
  - *Owsianik v. Equifax Canada Co.*, 2022 ONCA 813,
  - *Obodo v. Trans Union of Canada, Inc.*, 2022 ONCA 814, and
  - *Winder v. Marriott International, Inc.*, 2022 ONCA 815.
- All three decisions involved proposed class actions where:
  - The proposed class are individuals whose personal information was (or is alleged to have been) compromised in a data breach
  - The defendant is the company that handled and stored the personal information; and
  - The data breach was perpetrated by unidentified third-party hackers.
- Public Sector / Banking / FINTech all require you carry insurance against their data you hold in your system (PII / PHI) and that you take precautions against cyber attacks
  - Financial Organizations are regulated by OFSI, which has very specific regulations regarding cyber
- Often detailed in contracts with these bodies and is becoming more accepted in other sectors

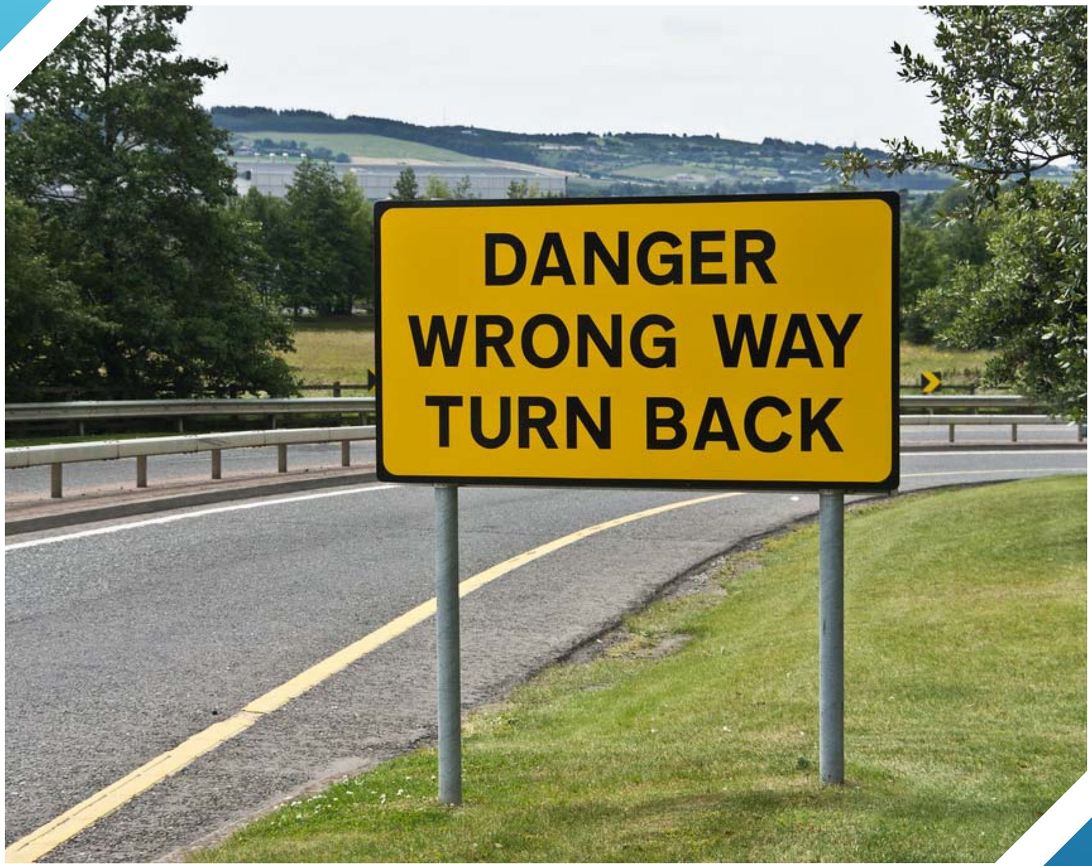
FINANCIAL IMPACTS

- Immediate impacts
  - Payout to threat actor
  - Cost of restoring clean data or sanitizing data
- Future impacts
  - Class action lawsuits
  - Remuneration for missing funds'
  - Credit monitoring
  - Increased insurance costs
  - Loss of business
  - Cost of more prevention
  - Legal costs
  - Public relations campaigns



SOCIAL AND PSYCHOLOGICAL EFFECTS

- Identity Theft
  - Stolen personal information can lead to fraudulent activities and financial ruin.
- Emotional Distress
  - Victims of cyber stalking, harassment, and fraud often suffer anxiety and fear.
- Workforce Morale
  - Employees working in breached organizations may feel insecure, affecting productivity.



OPERATIONAL DISRUPTION

- Cyber crime can paralyze an organization's operations, causing widespread disruption:
  - System Downtime
    - Malware and Distributed Denial of Service (DDoS) attacks can disable critical infrastructure, halting production and services.
  - Supply Chain Interruption
    - Attacks on logistics systems can delay shipments and disrupt manufacturing processes.
  - Data Loss
    - The corruption or theft of essential data can cripple decision-making and long-term planning.

PREVENTION & MITIGATION

Combating cyber crime requires a multi-layered approach:

- **Robust Cybersecurity Measures:** Firewalls, encryption, and intrusion detection systems form the first line of defense. Security standards and audit processes
- **Employee Training:** Awareness programs reduce the risk of phishing and social engineering attacks.
- **Incident Response Plans:** Preparedness minimizes downtime and accelerates recovery. Penetration testing is critical
- **Collaboration:** Sharing threat intelligence among businesses and government agencies strengthens collective defenses.

INTEGRATION WITH BC

- Process flow

1. Security group (or IT) identifies a breach
2. CISO is informed and analyzes the data (or directs the initial assessment)
3. The decision is made to inform your insurer
   - A. Insurer activates professional responder(s)
   - B. Responder contacts threat actor (if a cyber crime group)
4. Engineering / Database group begins to assess backups for cleanliness and begins restoration of data and applications from a clean backup or begins sanitizing data

The event will likely be run by a 3rd party used by your insurer, our job is to…

How would you build your response and recovery plan(s)?

KNOWLEDGE SHARING AND PLANNING IMPROVEMENT EXERCISE

- Let's divide up into groups and make note of ideas for how to improve our avoidance and response to cyber events
  - Prepare to present your 2 best ideas
    - Don't worry if another group mentions one of yours, you may have a different approach to how to implement

CONCLUSION