Chartered Governance Institute of Canada

Importance of Cyber Resilience

Hardeep Mehrotara

Chartered Governance Institute of Canada

Growing speed of Cyber Incidents

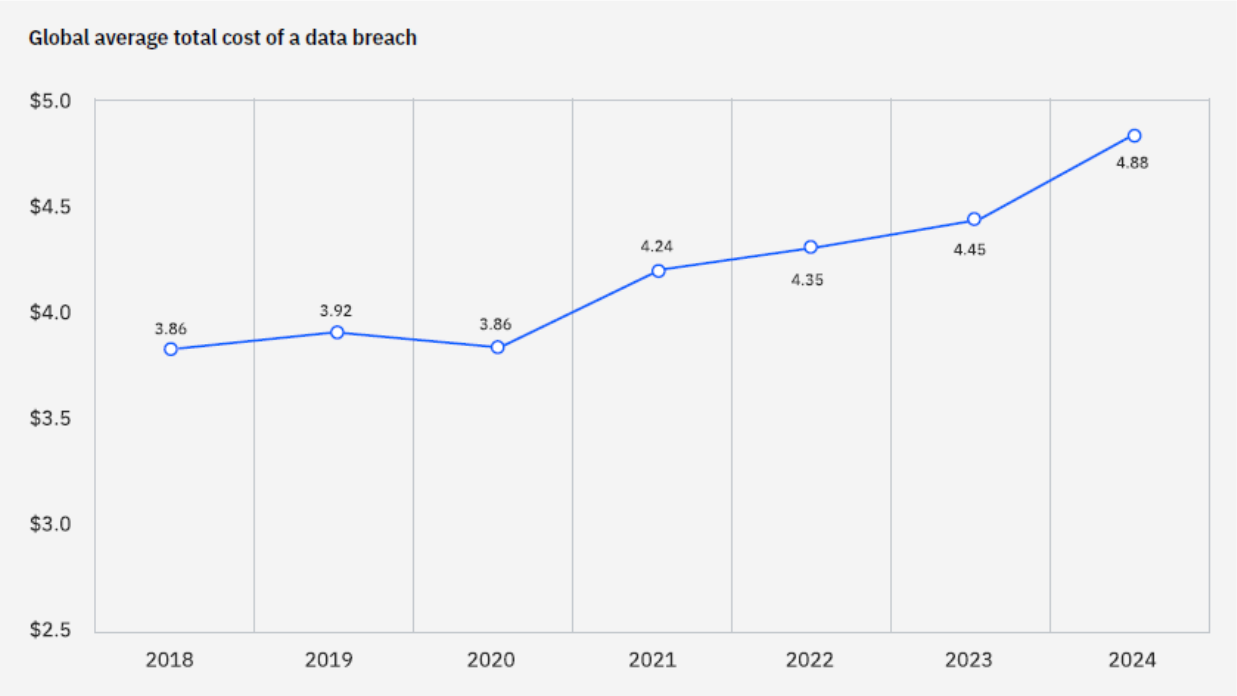


Figure 1. Measured in USD millions

- Cyber incidents are becoming more frequent and more sophisticated
- The cost of cyber incidents is increasing
- Organizations need to be prepared to respond to cyber incidents quickly and effectively

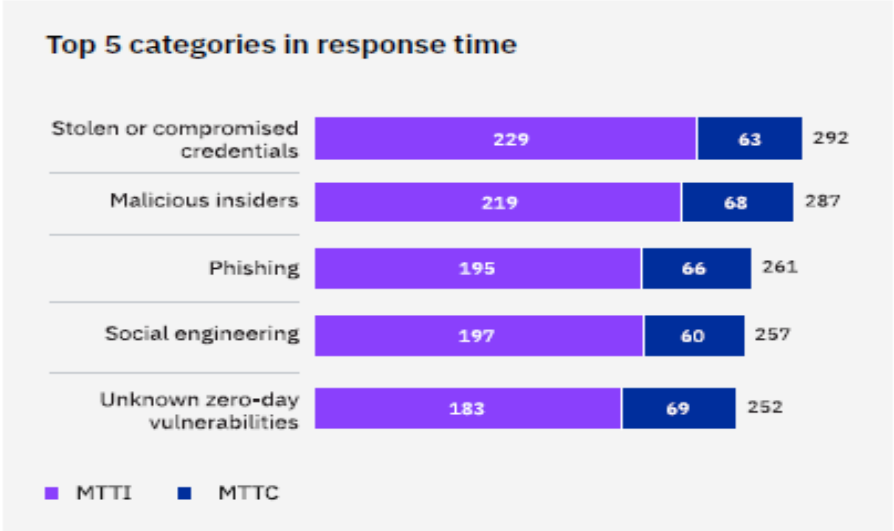


Figure 8. Measured in days

Chartered Governance Institute of Canada

Current Threat Landscape

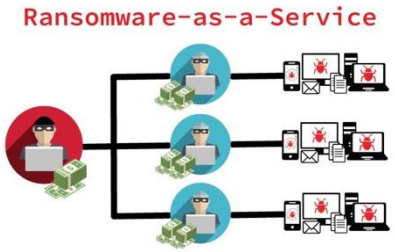
Artificial Intelligence and Deepfakes

Cyber criminals are using machine learning AI to generate phishing emails that are more authentic in nature and harder to detect.

ChatGPT and Deepfakes to initiate conversations with specific individuals within the company to gain access.

The speed and pace of attacks is increasing as cyber criminals are using automation.

Ransomware As a Service



Cyber criminals are providing Ransomware As a Service (RaaS) to make it easier for other cyber criminals to launch Ransomware campaigns and monetize profits.

Double or triple extortion efforts are being used along with Ransomware to force companies to pay and cash out.
Easier and faster rate of ransomware

Attacks against OT and IoT Networks

Cyber criminals are increasing their attacks against Operational Technology (OT) networks.

Devices such as building automation systems, access control, sensors are targeted.

Cyber criminals are using the weak controls in these networks to attack the rest of the company network.

Third Party Risk

Cyber criminals are studying companies to identify critical partners.

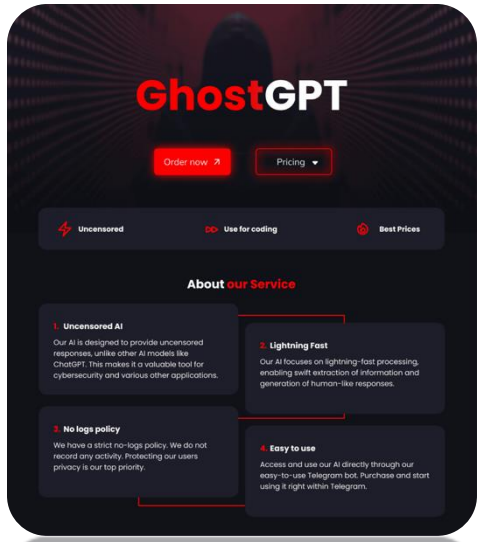
Partner networks are compromised to gain access or embed software which can later be used to gain access to the company network.

Chartered Governance Institute of Canada

Cybercriminals using AI

Types of AI Cyber Attacks:

- Iranian and Russian APT threat actors using Gemini.
- AI Phishing
- Deepfakes voice and video
- Developing and Deploying Malware
- Poisoning Machine Learning Algorithms
- Model Tampering
- Altered Malicious GPT

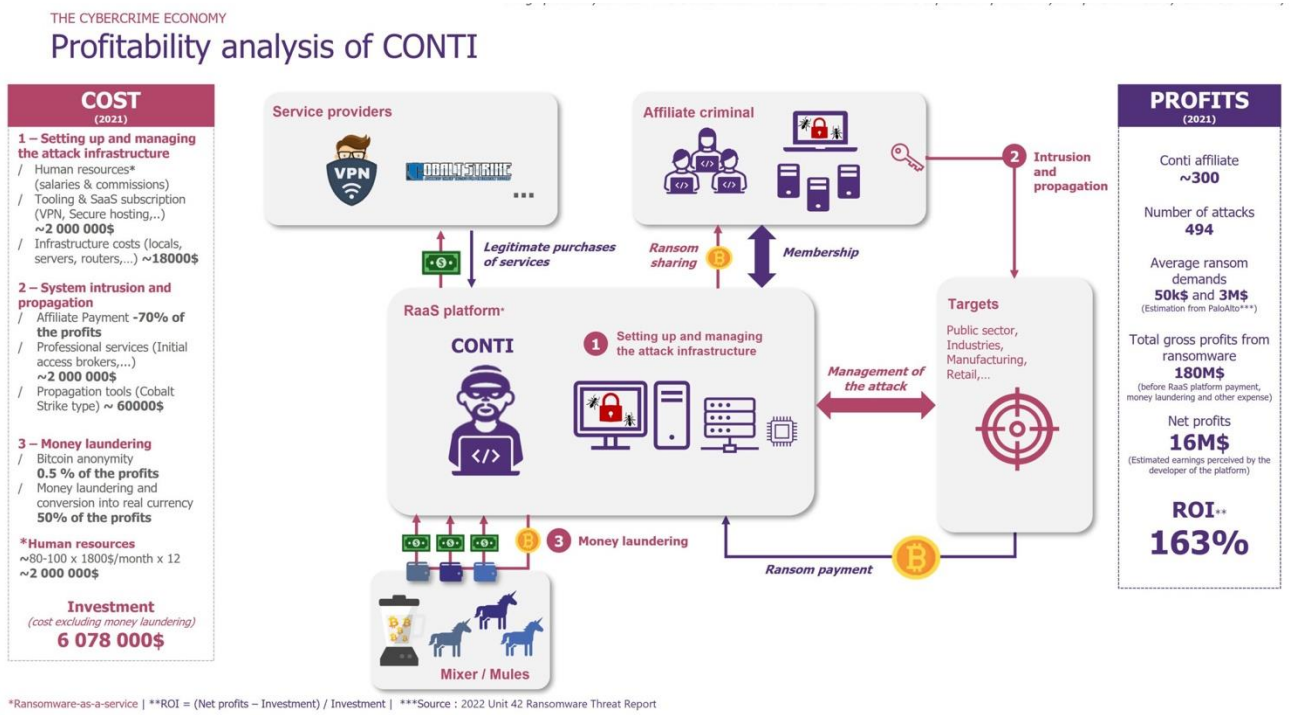


Chartered Governance Institute of Canada

Cybercriminals using Automation

Automation in Cyber Attacks:

- Attacks are faster and more coordinated.
- Attacks can be pointed to multiple sources (Websites, APIs, networks)
- Attackers can scale attacks against multiple victims simultaneously.
- Attackers can compromise and re-compromise.
- Malware can self-adjust based on the system.



Chartered Governance Institute of Canada

What is Cyber Resilience?

Cyber resilience is an organization's ability to prepare for, withstand, and recover from cyberattacks and disruptions, ensuring continued business operations and minimizing damage.

- Canadian Centre for Cyber Security – Transition to a cyber resilience approach
  - https://www.cyber.gc.ca/en/guidance/transitioning-cyber-resilience-approach-itsap10190

- National Institute of Standards and Technology - Cyber Resilience Systems
  - https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v2r1.pdf

Chartered Governance Institute of Canada

How do you achieve Cyber Resilience?

MINIMIZE THE IMPACT OF CYBER INCIDENTS

ENHANCE RECOVERY CAPABILITIES

MAINTAIN TRUST

ENSURE APPROPRIATE GOVERNANCE

ADAPT TO EVOLVING THREATS

Chartered Governance Institute of Canada

Minimize the impact of Cyber Incidents

- Data Protection
- Business Continuity
- Crisis Management

Chartered Governance Institute of Canada

Enhance Recovery Capabilities

Faster Recovery Times

Automation to reduce costs

Table tops & technical DR exercises

Risk Mitigation

Manage & maintain trust

Timely comms with Pre-defined holding messages

External PR firm

Social Media monitoring

Chartered Governance Institute of Canada

Ensure appropriate cyber governance

Board oversight

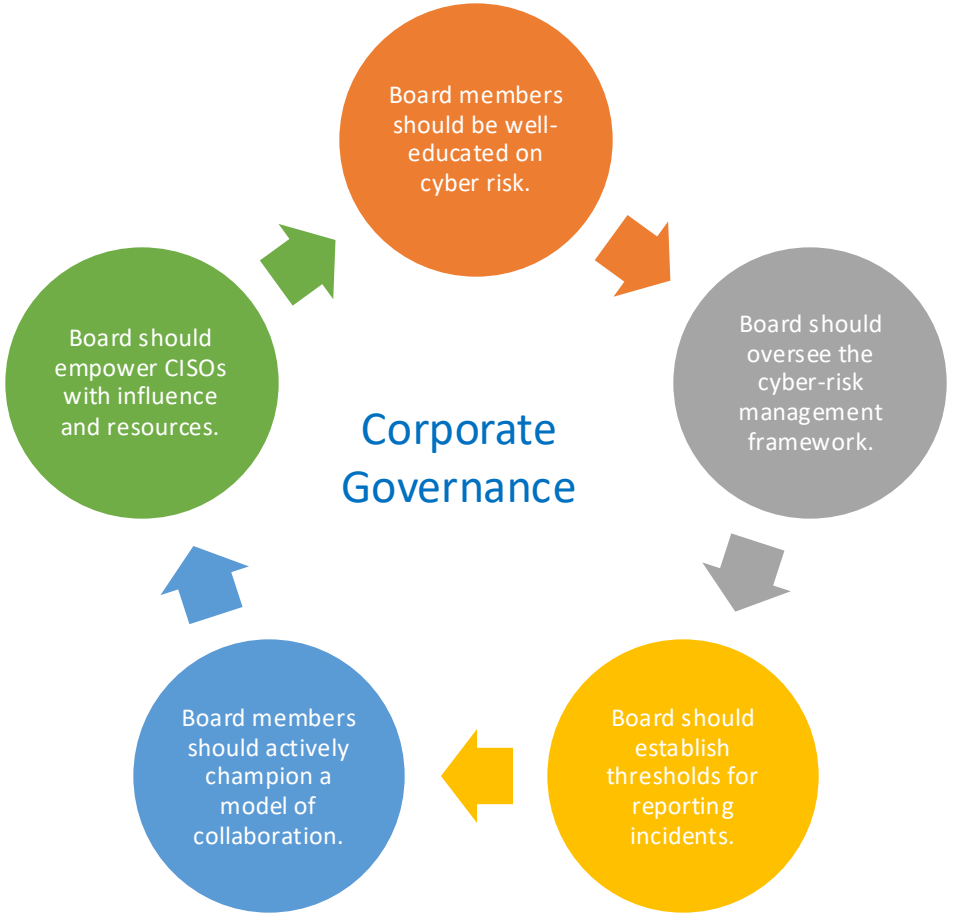
Annual assessment.

Compliance & Legal Obligations

Strong risk management practices.

Chartered Governance Institute of Canada

Board Oversight & Governance



Chartered Governance Institute of Canada

Adapt to evolving threats

Continuous Monitoring & Improvement

Employee Training

Strong network security & vulnerability Management practices

Threat Intelligence

Learning from Incidents

Regular testing and simulations (PenTest, Purple team, Red Team)

Chartered Governance Institute of Canada

Questions?