From Attack to Action: Navigating Cybersecurity in Retail Operations

LCBO

Neil Hopkins

Director, Cybersecurity

March 19, 2025

Agenda

1. The Cybersecurity Landscape in Retail
2. Threat Detection in Retail
3. Navigating and Mitigating Risks
4. Measuring the Impact of Cyber Incidents
5. Emerging Trends and Technology
6. Takeaways & Recommendations

Cybersecurity: Canada

By The Numbers

500+

Ransomware attacks in December

10+

Canadian Government websites targeted in December DdoS attacks

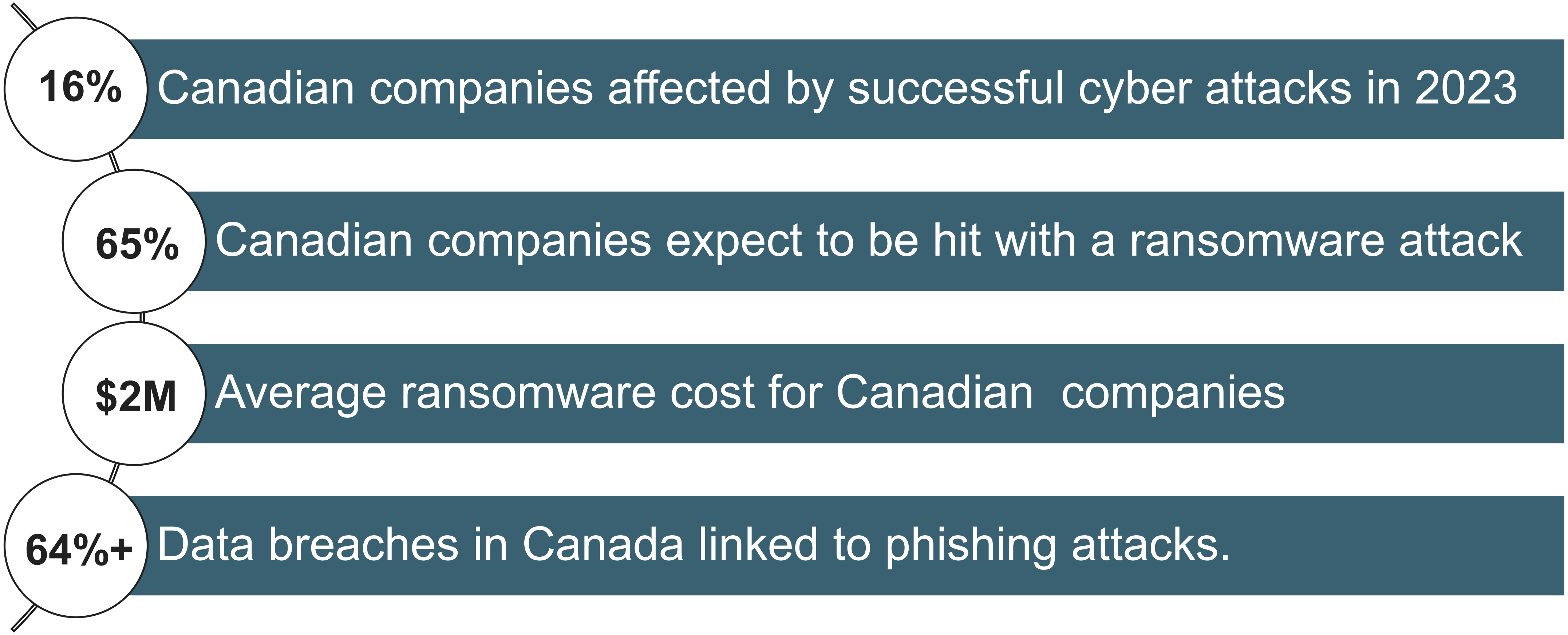
2.7B+

National public data breach impacting U.S., Canada & UK
(August 2024)

560M

Financial records from Ticketmaster breach
(May 2024)

Cybersecurity: Canada
By The Numbers



16% Canadian companies affected by successful cyber attacks in 2023

65% Canadian companies expect to be hit with a ransomware attack

$2M Average ransomware cost for Canadian companies

64%+ Data breaches in Canada linked to phishing attacks.

Cybersecurity risk in Retail:

By The Numbers

16% of ransomware attacks targeted food and beverage retailers

58% of attacks that originated from phishing

79% involved ransomware

92% of credentials were stolen from brute-force attacks

70% of attacks on retail sector led to customer data theft

LCBO

Source: Trustwave SpiderLabs Research: Defending the Retail Sector in 2024

Why Retail?

Customer Personally Identifiable Information (PII)

Financial Data

Hybrid brick and mortar & e-commerce

Implementation of new technologies

Threat Detection

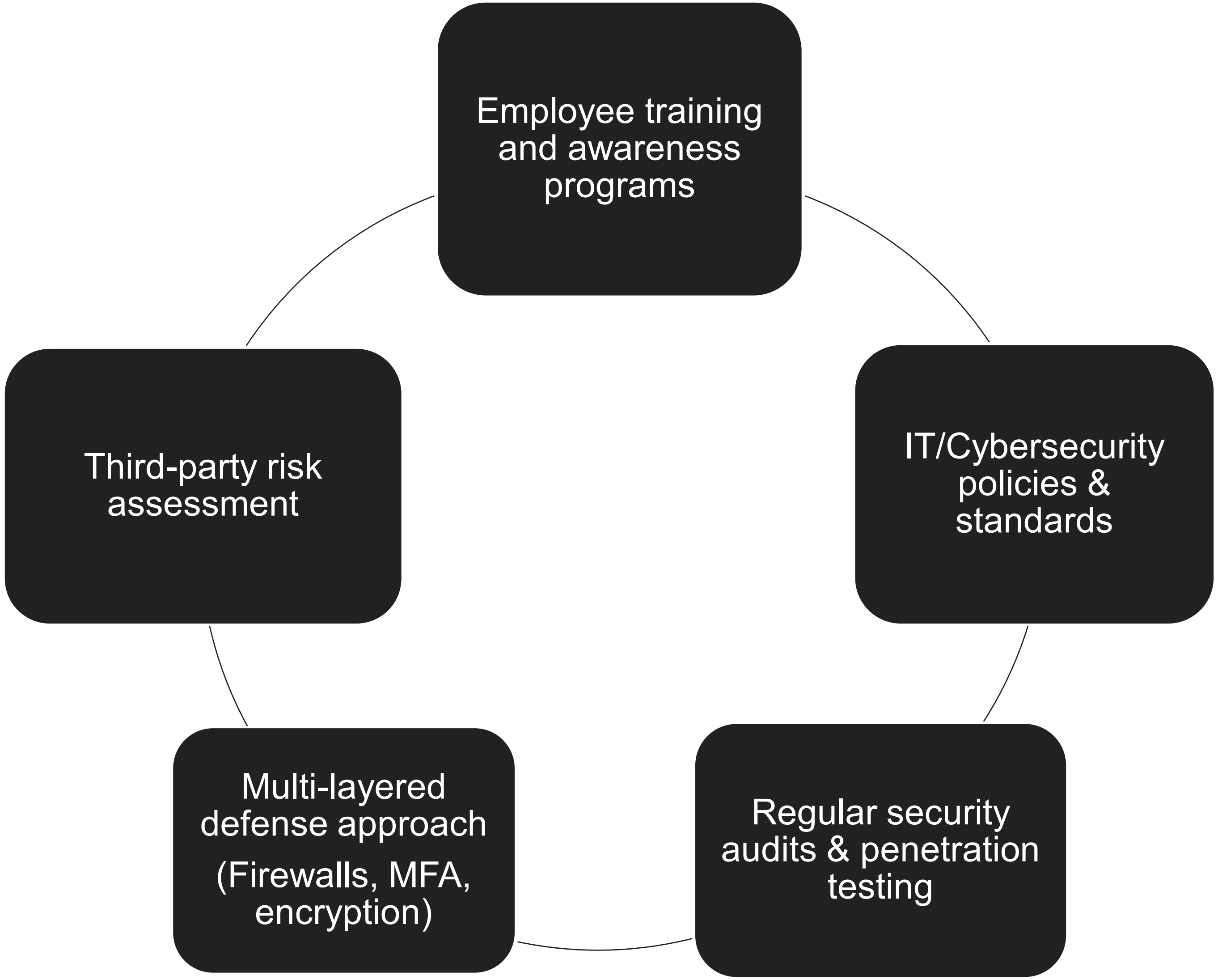
Effective threat detection strategies

- Implement real-time monitoring systems
- Enable logging
- Leveraging AI/ML for anomaly detection
- Endpoint security and intrusion detection systems (IDS/IPS)

Key Threat Indicators

- Suspicious network traffic
- Unusual user behaviour
- Data exfiltration attempts

Navigating & mitigating cyber risks



Employee training and awareness programs

IT/Cybersecurity policies & standards

Regular security audits & penetration testing

Multi-layered defense approach

(Firewalls, MFA, encryption)

Third-party risk assessment

Incident Response Planning

Complete regular tabletop exercises

Know your environment

Conduct business impact analysis

Review your incident response plan regularly

Set up out of band communications

Clearly define roles and responsibilities

Measuring the Impact of Cyber Incidents

Why impact measurement matters:

- Financial loss
- Brand reputation damage
- Regulatory fines and legal implications
- Reporting requirements

Measuring the Impact of Cyber Incidents

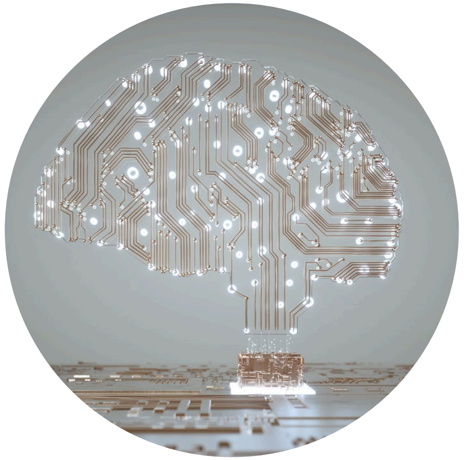
Metrics to measure impact

Downtime and recovery costs

Number of records compromised

Identification of critical assets

Emerging technologies



Artificial intelligence

Augmented & Virtual Reality

Smart checkout systems

Internet of Things (IoT)

Voice commerce

Key takeaways & Recommendations

- Understand your environment
- Complete business impact analysis
- Stay up to date with cyber
- Review your Incident Response Plan and cybersecurity policies
- Invest in technology, but with security in mind
- Invest in people and training

Thank you

LCBO