NORTON ROSE FULBRIGHT

Cybersecurity trends, cyber incident life cycle and preventative strategies

Alberta Municipalities - 2024 Public Risk Conference

John Cassell, Partner
Canadian Co-Head of Cybersecurity and data privacy

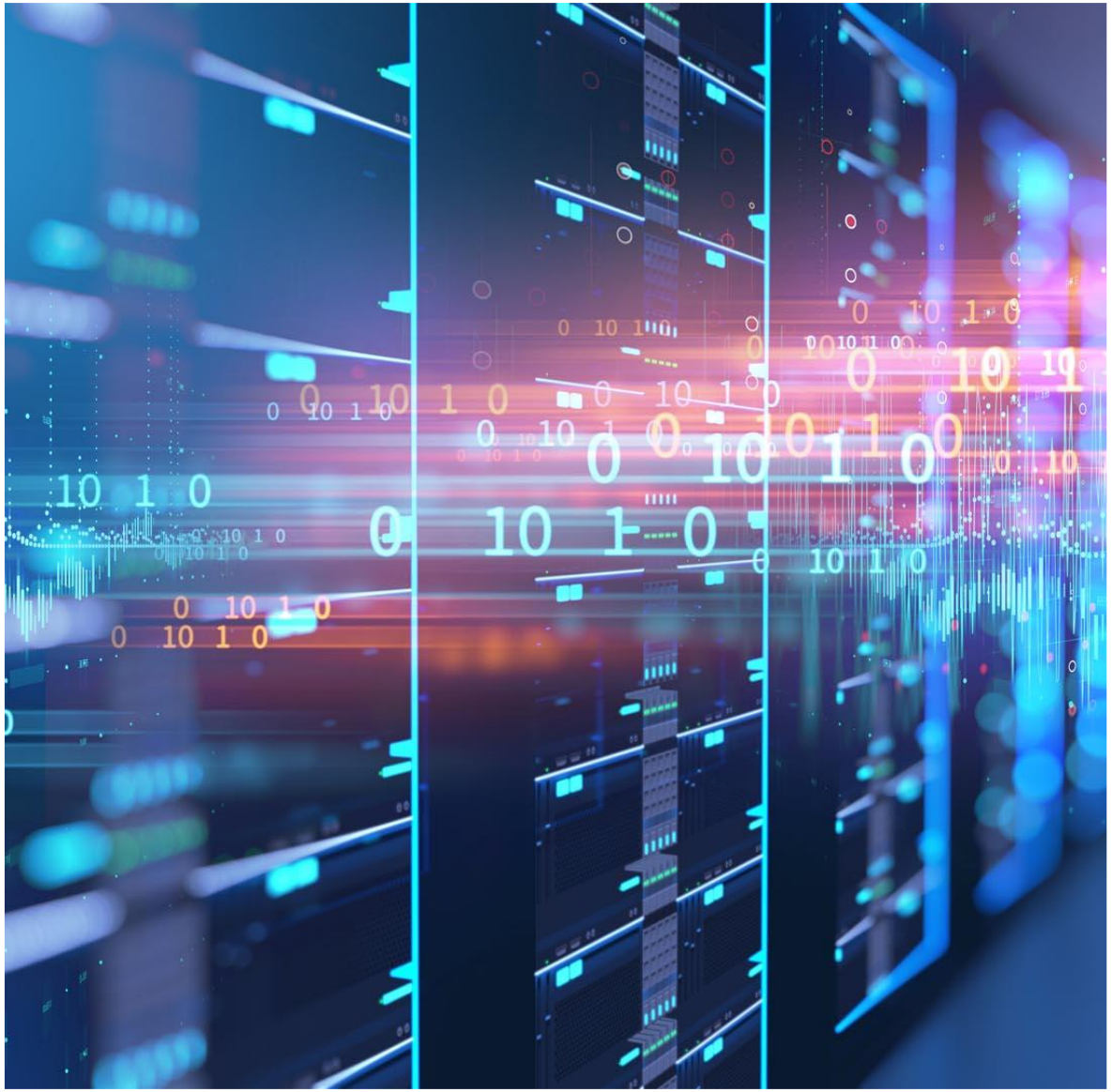
John Cassell

Partner, Canadian Co-Head of Cybersecurity and data privacy

John Cassell is co-head of Norton Rose Fulbright Canada LLP's information governance, privacy and cybersecurity team. John assists clients with all manner of privacy and cybersecurity law issues including: acting as breach counsel in responding to cybersecurity incidents, advising on cyber and privacy risk management strategies including pre-incident cyber-security preparedness and privacy/cyber vulnerability and gap assessments and assisting clients in responding to civil claims and regulatory investigations and enforcement actions arising out of a cybersecurity incident.

Agenda

- Cyber trends
- Breach Counsel Introduction
- Life-cycle of a cyber incident
- Cybersecurity preparedness strategies
- Legislative Updates



Overview of the Current Cyber Threat Landscape

- **According to IBM's Cost of a Data Breach Report,** the global average cost of recovery from a ransomware incident is $4.54 million USD.
  - Ransomware accounted for 11% of the types of breaches experienced by organizations in 2022.
- **Law enforcement takedown operations of prolific threat actor groups**
  - Blackcat (2023)
  - Lockbit (2024)

- **Attackers continue to employ dual and even triple extortion techniques:**
  - Data encryption ► operational disruption
  - Data theft ► sensitive data
  - Escalation tactics ► reputational harm
- **Quantum of ransom demands has materially gone up** (often between $2-10 million)
- **Challenge assessing value of data**
  - Personal information / personal health information
  - Sensitive corporate data
  - Sensitive third-party data
  - Cyber insurance considerations

Overview of the Current Cyber Threat Landscape

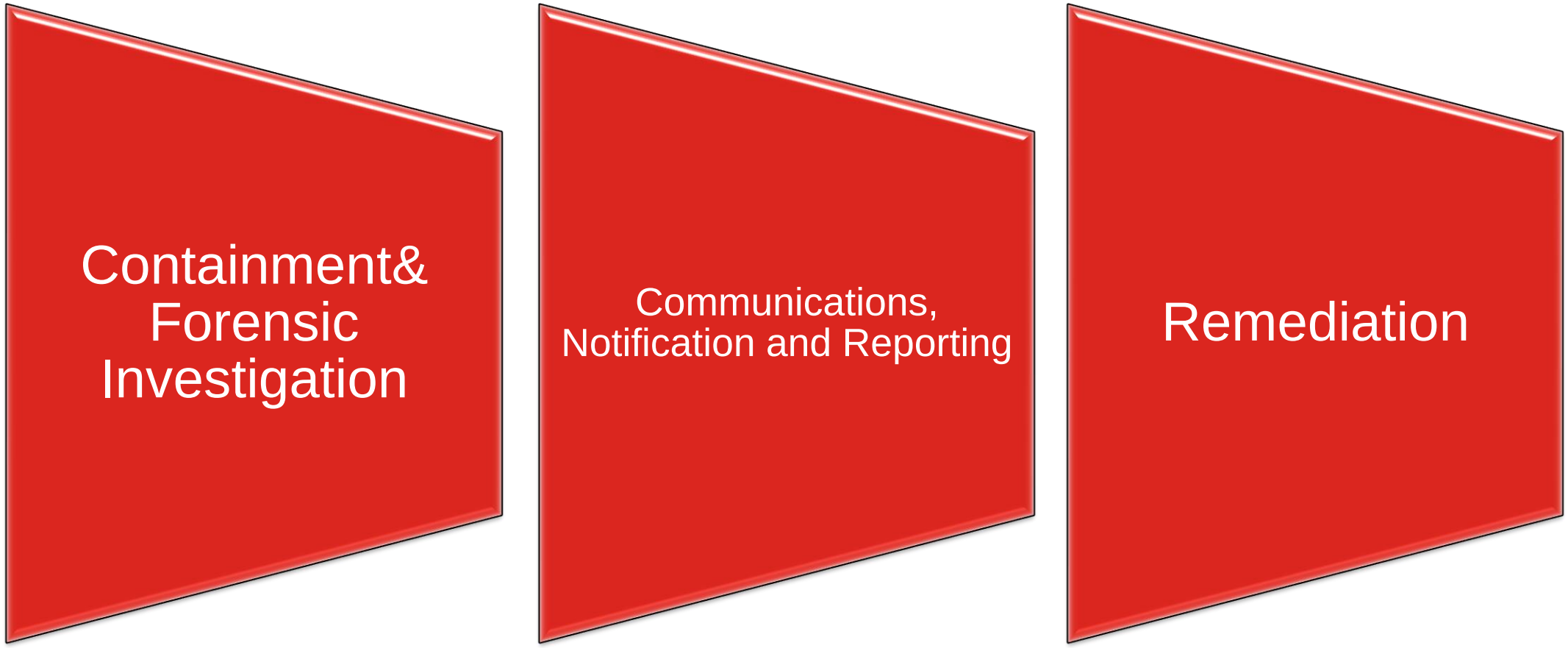
- **Ransomware attacks – remain prevent.**
  - Zero day vulnerability attacks
  - Significant third-party communication demands.
- **Business Email Compromise (BEC) and Social Engineering Scams**
- Heightened Sanctions Laws Compliance
  - Updated OFAC Compliance, Ongoing changes to Canadian sanctions laws
  - Directed at all organizations that assist organizations through an incident.

- **Potential for Operational Impacts/Business Interruption**
  - Sobeys (2022), Chapters/Indigo (2023), Suncor (2023), City of Hamilton (2024)
- **Nation State Intrusions** – Growing in frequency and severity, often with the aim of carrying out monitoring/profile building/IP theft.

Breach Counsel Introduction

- What does a breach counsel do?
  - Guide organizations through all elements of a data breach incident.
  - Breach counsel has unique perspective of being involved in all elements of the incident response. Assistance may include:
  - Retaining incident response vendors (forensics, ransom negotiator, communications, restoration, identity theft,
  - Directing privileged investigation into incident
  - Advising on legal requirements (reporting/notification)
  - Assists with communication strategy
  - Investigations and litigation arising out of incident
- Much of incident response work streams are confidential or subject to legal privilege and largely unknown

Responding to a Cybersecurity Incident

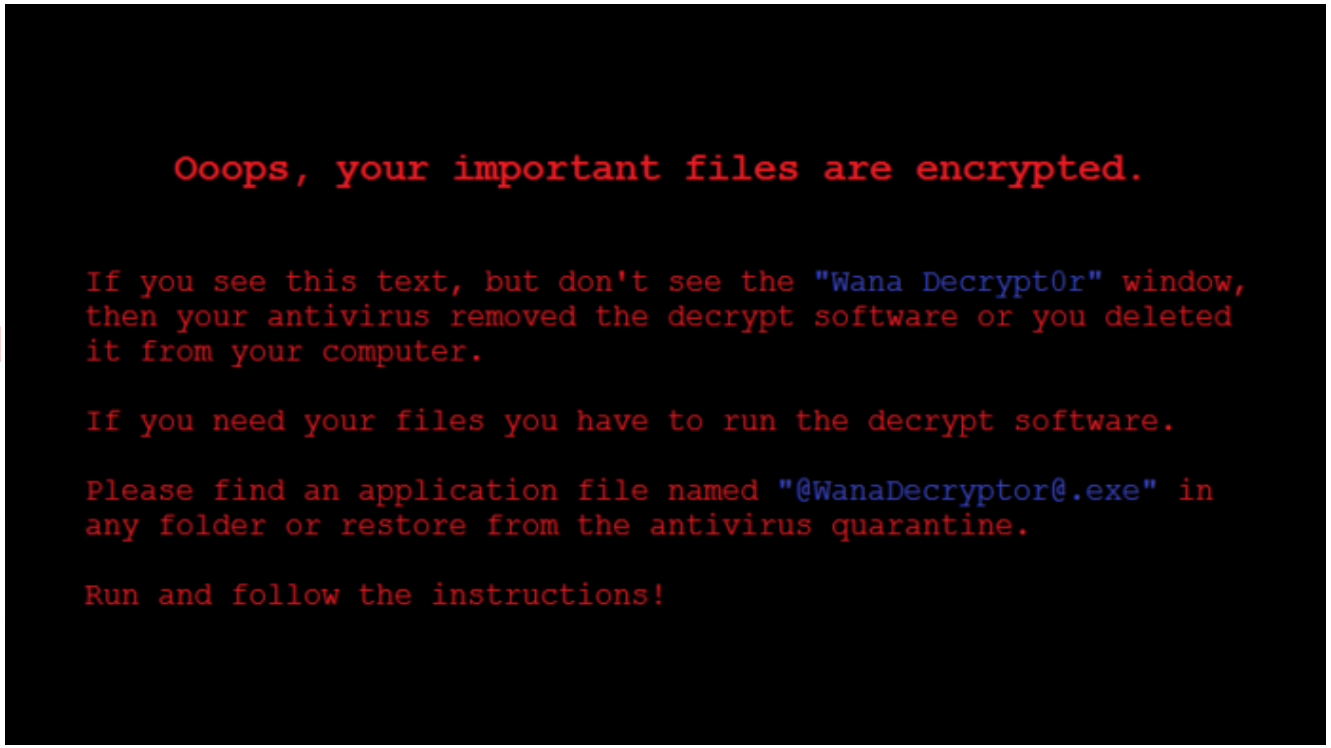


Containment

- Engagement of incident response and forensic experts by Breach Counsel under privilege
- Direction of privileged forensic investigation
  - Creation of incident response SOW
- Initial Breach counsel considerations during containment phase:
  - Scope of Incident - What systems are impacted?
  - Ransom note? (Do not engage the threat actor!)
  - Evidence of data exfiltration/theft ?
  - Operational Status?
  - Attack vector known?
  - Immediate containment steps possible?
- Coordination of Incident Response and Restoration teams critical

Ransomware Negotiations

- Decision to commence negotiations requires multi-factored analysis
  - Depends on ongoing results of forensic investigation, operational status, ransom demands, etc.
- Ransom note will not contain ransom demand. Required to click on link to commence negotiations.
- Relevant Questions:
  - Data encrypted?
  - Back-ups available/viable?
  - Evidence of data exfiltration?
  - What type of data potentially exfiltrated
  - Amount of ransom demand?
  - Status of ransom demand / deadline?
  - Additional time needed?
  - History/reliability of threat actor
- Case Study Examples



Ransomware Negotiations

- Third party firm cyber extortion firm retained by breach counsel to conduct ransom negotiations.
- “Proof of Life” process
  - Initial phase of negotiations.
  - Proof of Data Exfil - Involves requiring threat actor to provide file tree/file list of data stolen. Opportunity to choose several files from list.
  - Proof of Decryption – provide (non-sensitive) encrypted files to TA. TA typically provides back unencrypted files.
- Common strategy to commence negotiations for sole purpose of gaining visibility/evidence of data exfiltration.
- Depending on TA, escalation tactics/harassment may be utilized to pressure commencement of negotiations or settlement.
- Cadence of communications, size of discounts, timeline for negotiations largely dictated by TA.

Ransomware – Facilitating Payment

- Confirmation of terms of agreement with Threat Actor. Typical standard Agreement Terms
  - Decryption key (windows and linux if applicable)
  - Proof of deletion of exfiltrated data
  - Agreement to not post organization name on TA leak site
  - Promise to not attack organization again
  - “security report” (how the TA “got in”)
- Facilitation of ransom payment
  - Payment via digital currency (Bitcoin, Monero)
  - Payment in CDN or USD is made to ransom negotiation firm who in turn purchases bitcoin.
- Sanctions Laws Compliance
  - OFAC, Canadian sanctions laws

Engagement with Law Enforcement

- Early reporting recommended to law enforcement
  - Reporting to local law enforcement and/or RCMP, coordination with FBI
  - Insurance requirement
  - Positive communication messaging
- Reporting required for OFAC compliance with anticipated ransom payment
- Information sharing with law enforcement
  - Client concerns regarding maintenance of confidentiality/legal privilege
  - Information included as part of disclosure package
  - Potential “easy win” deliverables
    - IOCs, ransomware variant, ransom note, intelligence sharing
- Reporting necessary for potential ransom payment restitution
- Law Enforcement proactive notification of clients regarding incidents

NRF

Communications

- Crisis communications critical component of effective incident response
- Breach counsel involved as part of communications team. Incident response team may include members from various departments (Human Resources, IT, Communications, Operations, Legal, Management)
  - Incident response communications not only an IT issue
  - Internal communications teams under-utilized
- Crisis management – speed key
- When to acknowledge breach/cyber-security incident?
  - Control the message/narrative until key facts are known
  - Reactive preparation key – communication playbook/materials
- Customer/Stakeholder communications
  - Increased scrutiny from customers requires coordinated response
  - Consider dedicated customer resources, involve account managers/stakeholders
  - Prepare for common customer requests: statement of containment, root cause analysis (RCA), IOC's, impact to data

Forensic Investigation

- Typically conducted by third party forensic firm at the direction of legal counsel
- Importance of maintaining privilege over investigation and reports
  - Be mindful about relying on existing service agreements – enter into a new statement of work/agreement related to the specific incident at hand
- Scope of forensic investigation typically includes:
  - Root cause of incident
  - Attack vector
  - Data exfiltration / unauthorized access
  - Remediation recommendations (included in separate report)
- Limit sharing of forensic report regarding
  - Requests from auditors, customers, vendors, other third parties
  - Consideration of other avenues to provide responses

Notification and Reporting

Canada

- Personal Information Protection Electronic Documents Act (PIPEDA) / Personal Information Protection Act (Alberta)
  - "Breach of security safeguards" resulting in a "real risk of significant harm" to affected individuals

- Freedom of Information and Protection of Privacy Act (FOIP) (Alberta)
  - "public bodies" are not required by law to notify the Alberta OIPC of privacy breaches although they are nonetheless recommended.
- Bill 64 (Quebec)
  - Significant changes to privacy landscape in Canada
  - **September 2022**: Obligation to notify regulator and individuals of data incidents if risk of harm
  - Businesses must appoint a person in charge of the protection of personal information: responsible for ensuring legal compliance
  - **September 2023**: Increased penalties and fines – up to $25,000,000 or 4% of worldwide revenue

Notification and Reporting

Canada (Continued)

- Bill C-26 – Cyber Breach Reporting Requirements
- Bill C-27 – Amendments to PIPEDA

International requirements

- General Data Protection Regulation (GDPR)
- US state requirements

Other notification obligations

- Contractual notice requirements
- Governmental bodies/departments

Coordinated approach to notification / reporting

- Regulatory reporting typically made prior to individual notifications
- Contractual notice requirements

Remediation and Recovery

- Make recommended technical security improvements/fixes post-incident
  - Remediation report separated from forensic report
  - Installation of Endpoint Detection Monitoring (EDR) Tools
  - Implementation of Multi-Factor Authentication (MFA)
  - Data-mapping initiatives
  - Data-retention review (data purging)

- Assessment and improvement of incident response plan
  - Review of incident-detection triggers

- Conduct post-incident organizational assessment

Pre-Breach Planning & Cyber-Security Preparedness

- **Previously**: “Not if, but when”. **Now**: “Not when, but how many”
- Implementation and/or review and update of Incident Response Plan
  - Include specific plans for ransomware
- Table-top exercises
- Data mapping assessments
- Pre-onboarding of Incident Response Vendors
- Employee privacy and cybersecurity training and awareness
- Ongoing review and improvement of technical safeguards (Penetration testing, gap/vulnerability assessments)
- 3rd party vendor risk management program

NRF

Pre-Breach Planning & Cyber-Security Preparedness

Previously: “Not if, but when”. **Now**: “Not when, but how many”

Cyber Incident Response Plan (CIRP)

- Developing a CIRP assist with speed and effectiveness of response in the event of a cyber incident which ultimately assists in minimizing damages/loss from the Incident.
- Key Elements of a CIRP:
  - Simplicity and Role-Specific
  - Pre on-boarding of Incident Response Vendors
  - Add Insurance Contacts
  - Playbooks (Ransomware, Business Email Compromises)
  - Protection of Legal Privilege
  - Triage/Detection of Incidents
  - Coordination with other Incident Response/Emergency Plans
  - Third-party cyber incidents
  - CIRP contemplates OT environment?

NRF

Pre-Breach Planning & Cyber-Security Preparedness

Tabletop Exercises/Cyber-Security Simulation

- Simulation of cyber-security Incident
- Table-top exercises are designed to test communication, decision-making and responding to an Incident.
- Tests effectiveness of a CIRP – make improvements to the CIRP following the tabletop exercise.
- Ensure individuals from different departments/business units involved
- Technical tabletop exercises v. management-focused
- Board Education/training
- Perform tabletop exercises annually

Information Governance/Privacy Compliance Program

- Privacy compliance foundational element of cyber-security program
- Cyber-security incidents increase risks associated with privacy law non-compliance
  - Risk of investigations, compliance orders by privacy regulators, fines, civil actions

NRF

Pre-Breach Planning & Cyber-Security Preparedness

Third Party Vendor Management Program

- Third party vendors can potentially represent a significant risk from a cybersecurity and privacy perspective.
- Organizations remain contractually responsible for data transferred to third parties - critical that a process is established during vendor onboarding process and during term of relationship relationship to screen and monitor cyber risks to allow for proper mitigation
- Tailored use of contractual provisions (through data protection addendum) to address identified cyber-risks.
- Use of audit and compliance provisions to monitor compliance.

Pre-Breach Planning & Cyber-Security Preparedness

- **Data-Mapping/Data Inventory Exercises**
  - Identification of types of data collected, repositories of data, data paths
  - Application of appropriate security safeguards
  - Data retention/data purging
- **Technical Security Safeguards**
  - Numerous technical security safeguards that form part of a robust, effective cyber-security program – (ie. Multi-factor authentication, End Point Detection and Monitoring Software, patching program, backup systems)
  - Technical safeguards tested through regular penetration testing/vulnerability assessments.
- **Cyber Key Performance Indicators (KPI's)**
  - Track KPI's regarding cyber-security at the board and executive level.
  - i.e. number of confirmed cyber-security "Incidents", average incident response time

Legislative Updates

Bill C-26

- *An Act Respecting Cyber Security, Amending the Telecommunications Act and making consequential amendments to other Acts*
  - Amendments to *Telecommunications Act*
  - *Enactment of Critical Cyber Systems Protection Act (CCSPA)*

Bill C-27

- Enactment of *Consumer Privacy Protection Act* (CPPA), *Data Protection Tribunal Act* and *Artificial Intelligence and Data Act* (AIDA)
- Significant overhaul of Canada's federal privacy legislation (PIPEDA)
  - Significant fines and penalties for non-compliance (fines as a percentage of global revenue), legal claims for breaches of privacy
  - Creation of New Data Protection Tribunal
- The *Artificial Intelligence and Data Act* (AIDA) is Federal Government's first attempt to regulate AI.

Legislative Updates

Quebec's new Bill 64 adopted in September 2021 – Law 25

- New obligations coming in 2022, 2023, 2024
- Only applies to information that can be used to identify individuals

- September 2022
  - Obligation to notify regulator and individuals of data incidents if there's a risk of harm
  - Businesses must appoint a person in charge of the protection of personal information: responsible for ensuring legal compliance
- September 2023
  - Develop and publish data protection and confidentiality policies
  - Assessment of privacy related factors
  - Increased penalties and fines – up to $25,000,000 or 4% of worldwide revenue
- September 2024
  - Data portability rights

NRF

Law around the world

nortonrosefulbright.com