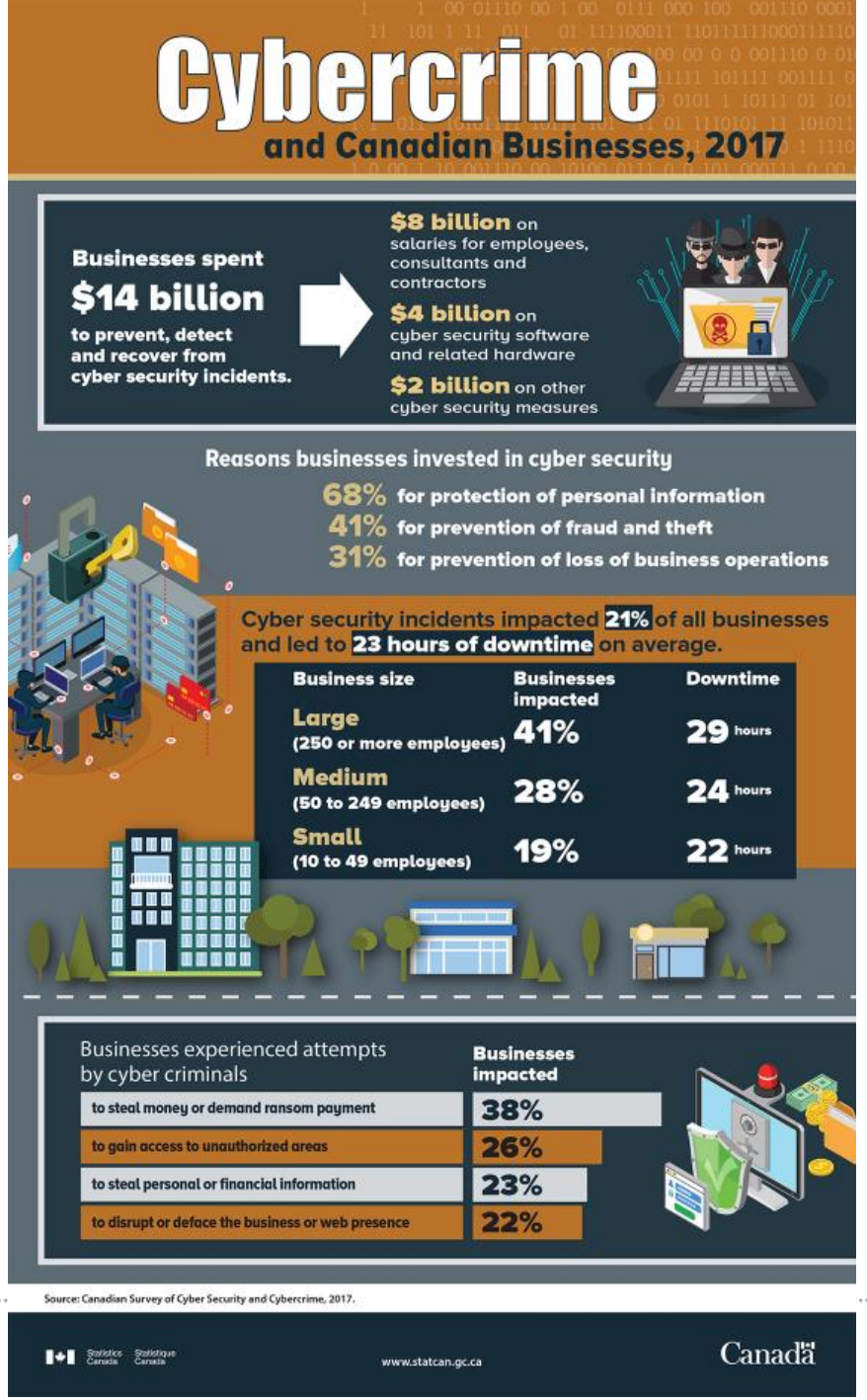
STEWART McKELVEY
LAWYERS • AVOCATS

Cyber-liability and Privacy:
Cyber Security Matters

Koren Thomson
Sarah Dever Letson

Cybersecurity attacks – what are the numbers in Canada?



Source: StatsCan Canadian Survey of Cybersecurity and Cybercrime, 2017 (released Oct. 2018)

Scalar Security Study 2019:

- 100% of surveyed organizations had experienced a cyber security attack over the past 12 months
- 58% had data exfiltrated
- Overall number of attacks declined from 455 (2018) to 440 per organization
- Cost per organization of responding to and recovering from cybersecurity incidents increased from $3.7 million to over $4.8 million – this is primarily tied to the length of detection and response time
- The security strategy of the Canadian organizations is shifting from protection to detection and response

Recent high profile cyberattacks in Canada:

- Equifax – personal information of approx. 19,000 Canadians was accessed
- Bell Canada – hackers gained unauthorized access to personal information of 100,000 customers
- Ransomware attacks on municipalities – Midland and Wasaga Beach, Ontario
- Saint John Parking Commission

What is at risk from a cyberattack?

CYBER risk = risk

- Business disruption
- Loss of confidential business information, including financial and IP information
- Loss of employee or customer personal information, including credit card information
- Reputation
- Regulatory infractions/prosecutions
- Privacy complaints
- Litigation

What are Canadian organizations doing about cybersecurity?

StatsCan Canadian Survey of Cybersecurity and Cybercrime:

- 95% of Canadian businesses employ some form of cybersecurity to protect themselves, their customers and their partners in 2017
- Approximately one-third (29%) of businesses were required to implement cybersecurity measures by their suppliers, customers, partners or regulators
- Almost one-quarter (24%) of large businesses indicated that they had cyber liability insurance to protect against cybersecurity risks and threats, compared with 14% of medium-sized businesses and 7% of small businesses

CIRA/Strategic Council Cybersecurity Report 2018:

- 59% said they stored personal information from customers, but only 38% said they were familiar with PIPEDA
- 34% mostly relied on vendors to handle their cybersecurity needs, 33% felt they had an equal mix of insourced and outsourced resources, while 27% reported internal resources only

What is the law on Cybersecurity?

Legislative framework:

PIPEDA

- Privacy designate
- Policies and practices
- Appropriate security safeguards
- Breach reporting and notification requirements
- Breach documentation requirements

Legislative framework:

PIPEDA – Consent requirements

- Consent is valid if it is reasonable to expect your customers would understand the nature, purpose and consequences of the collection, use or disclosure they are consenting to
  - Tell customers what you are collecting and why
  - Tell them in a meaningful way, the purpose of the collection, use or disclosure
  - Obtain consent before or at the time of collection, AND when a new use of the personal information is identified
- Exception: Witness statements

Legislative framework:

Legislation protecting personal health information

- Provincial legislation existing in all jurisdictions.
- Contains limitations on the collection, use, and disclosure of personal health information by custodians, as well as requirements for security safeguards and mandatory breach reporting.

Legislative framework:

Provincial access to information legislation

- Provincial legislation existing in all jurisdictions – applies to government departments, municipalities, universities.

- Contains limitations on the collection, use, and disclosure of personal information, as well as requirements for security safeguards and mandatory breach reporting.

Legislative framework:

Criminal Code - Cyber criminal offences include:

- Using a device willfully to intercept a private communication without the express or implied consent of the originators or intended recipient (s. 184); and
- Intercepting fraudulently any function of a computer system (s. 342.1).

Legislative framework:

Canadian Anti-Spam Law ("CASL")

- Prohibits installation of computer programs on another person's computer system without the express consent of the owner or an authorized user of that system.
- Prohibits causing computer program to communicate with other electronic devices without consent.
- Applicable if installer or target computer system are in Canada.

Legislative framework:

General Data Protection Regulation ("GDPR")

- Has application to some Canadian organizations.
- 72 hour breach notification requirement

Legislative framework:

- Sector specific statutes, e.g. *Bank Act*

- Bill C-59 – if passed, will create the *Communications Security Establishment Act*, and grant new powers to defend critical Canadian infrastructure (telecommunications, nuclear plants) from attacks, and launch cyberattacks.

- There is also sector specific regulatory guidance, including from Sector specific regulatory guidance, including from IIROC, Canadian Securities Administrators and MFDA.

What type of litigation?

Claims for breaches of statute

- There is no independent cause of action for breach of statute (*R v Saskatchewan Wheat Pool*, [1983] 1 SCR 205).

- Legislation may inform negligence analysis.

Civil causes of action

- Breach of Contract: arising from failure to satisfy contractual obligation to protect information.
- Negligence: arising from failure to employ sufficient safeguards.
- Intentional Torts: generally arising from employee snooping or harvesting of data for sales.

Intentional torts

Intrusion Upon Seclusion

(a) Intentional conduct (includes reckless conduct);

(b) That invades a person's private affairs or concerns without lawful justification;

(c) That a reasonable person would regard as highly offensive, causing distress, humiliation or anguish.

Statutory Torts

(a) A violation of an individual's privacy;

(b) That is done willfully; and,

(c) That is done without a claim of right.

Class actions

- Lost or misplaced information (I.E. *Condon*)
- Employee snooping (I.E. *Hemeon*)
- Employee stealing information for 3rd parties *(Evans v BNS*)
- Third party hacking (*Home Depot*)

Exposure impacted by:

- Breach response & mitigating efforts
- Type of information at issue
- Risk of misuse/harm
- Number of people impacted

Vicarious liability for cybersecurity matters

- VL imposed when act is authorized or the act is so connected with authorized acts that they are regarded as a mode of doing an unauthorized act (*Bazley v Curry*, 1999 CarswellBC 1264 (SCC).

- The problem of the “Rogue Employee”.

- *Various Claimants v WM Morrisons Supermarket PLC*

Other sources of civil liability

- Claims by financial institutions
- Claims by shareholders

What about insurance?

Potential applicable policies

- Commercial general liability
- Errors and omissions
- Director & officer liability

Oliveira v Aviva Canada Inc.

- Breach of privacy at hospital by hospital employee.
- Aviva insured hospital under Professional and General Liability and Comprehensive Dishonesty, Disappearance and Destruction Policy.
- Employees were additional insureds where acting on the direction of the hospital and only in respect of liability arising from the operations of the hospital.
- Aviva characterized the employee as a “rogue” employee to whom it did not owe a duty to defend.
- The Court disagreed. Its decision was upheld by the Ontario Court of Appeal.

Cyber Security Insurance

- Policies for losses resulting from cyber security incidents
- Very little standardization
- What may not be covered:
  - Social engineering losses
    - *The Brick Warehouse LP v Chubb Insurance Company of Canada*, 2017 CarswellAlta 1208 (ABQB)
  - New hardware

- Software upgrades
- Third-party errors
- Third party contract claims
  - *P.F. Chang's China Bistro Inc v Federal Insurance Company*, 2016 WL 3055111
- Intellectual property theft and reputation damage

So what is covered?

- First party coverage
  - Notification costs
  - Forensic investigation costs
  - Crisis management costs
  - Cyber extortion costs
- Third party coverage
  - Network security costs
  - Privacy liability

What is effective cybersecurity governance?

- Increased cost of Cybersecurity attacks is resulting from detection and response times being too slow

- Deficiencies in planning for incident response leaves organizations vulnerable if there is a breach

- Directors of Canadian companies, consistent with their fiduciary duty and duty of care, need to exercise oversight over cybersecurity risk

- Liability can arise not from a cybersecurity breach itself, but from a failure to demonstrate that the board properly assessed and considered the risk.

- The bottom line is – the development of appropriate policies and procedures to manage and address cybersecurity risk can demonstrate board care and diligence.

Development of a Cybersecurity plan:

Audit of assets and risks:

- Identify types and location of assets/information;
- What is the most valuable and the most vulnerable?
- Compliance requirements
- Industry standards (i.e, encryption, multi-factor authentication)?

Development of a Cybersecurity plan:

Audit of assets and risks:

- IT and other systems infrastructure
- Current processes and procedures
- Use of third party suppliers/vendors
- Employees
- Collection/retention policies.

Components of a cybersecurity plan:

Source: IIROC Cybersecurity Best Practices Guide

Components of a cybersecurity plan:

- Security safeguards/defensive plan
- Breach detection/monitoring
- Breach response
  - Response team (GC, IT/forensics, communications, board representative)
  - Preservation of evidence/records
  - Documentation of breach

Components of a cybersecurity plan:

- Breach Response (cont'd):
  - Identifying threshold for notification;
  - Notification procedures.

- Breach Recovery

- Organization and board buy-in:
  - Responsibility
  - Budget
  - Education
  - Training
  - Regular reporting to the board.

- Regular review:
  - # of incidents and response;
  - Security safeguards, technical infrastructure (updates, patches);
  - Breach response plan;
  - Testing of breach response plan;
  - Third party and supplier risks;
  - Risks associated with employee conduct;
  - Scope of cyber insurance

Questions?

STEWART McKELVEY
LAWYERS • AVOCATS

Nutrition Break (2:10-2:25pm)

Food and Beverage Area

Dr. Allan Abbass: "Evaluation and Treatment of Emotional Factors in Somatic Presentations" (2:25pm-3:25pm)

Argyle Suite

STEWART McKELVEY
LAWYERS • AVOCATS

These materials are intended to provide brief informational summaries only of legal developments and topics of general interest.

These materials should not be relied upon as a substitute for consultation with a lawyer with respect to the reader's specific circumstances. Each legal or regulatory situation is different and requires review of the relevant facts and applicable law.

If you have specific questions related to these materials or their application to you, you are encouraged to consult a member of our Firm to discuss your needs for specific legal advice relating to the particular circumstances of your situation.

Due to the rapidly changing nature of the law, Stewart McKelvey is not responsible for informing you of future legal developments.