



mccarthy
tetrault

Cybersecurity Risk Management

A Practical Guide for Businesses


**mccarthy
tetrault**

Table of Contents

01. Cybersecurity Risks and Advantages	1
More Data	1
Larger and More Complex Data Incidents.	1
More Costly Data Incidents.	2
From Compliance to Competitive Advantage.	2
02. Why Cybersecurity Preparedness Matters	3
Better Outcomes	3
Evolving Standard of Care.	3
03. Cybersecurity Preparedness and Incident Response Plan	5
Cybersecurity Framework	5
Governance	5
Actions of Directors and Officers.	6
Training and Policies	6
IT Security.	6
Acceptable Use and Use of IT Assets	6
Employee Education and Training	7
Vendor Due Diligence.	7
Third Party Access and IT Service Agreements	8
IT Security, Malware and Monitoring	9
Examples of Vendor Due Diligence Inquiries	9
Cybersecurity Risk Insurance	9
Examples of Cybersecurity Risk Insurance Considerations.	10
Cybersecurity Incident Response Plan	11



04. What To Do When the Worst Happens:	
Executing the Cybersecurity Response Plan	13
Contain the Incident	13
Convene the Team.	14
Legal/Compliance	14
Public Relations/Marketing	15
Customer Care	15
Human Resources.	15
Corporate Security/Risk Management.	15
IT.	15
Analyse and Document the Incident.	15
Competencies of an IT Forensics Firm	16
Assess and Manage the Legal Implications	17
Regulatory Risk	19
Insurance Coverage	19
Law Enforcement	21
Consumer/Customer Response	21
Prepare and Send Reports to Commissioners and Notices to Affected Individual	23
Notification to Privacy Commissioner(s)	23
Notice to Affected Individuals	24
Record Keeping Obligations.	25
International Considerations	26
Meet Specific Industry Requirements.	26
Healthcare	26
Payment Cards.	26
Public Companies.	28
05. Helping You Prepare and Respond.	33



This article is for general information only and is not intended to provide legal advice. For further information, please speak to one of your McCarthy Tétrault contacts.

01



Cybersecurity Risks and Advantages

Where there is data, there is the potential for data loss. How an organization prepares for and manages a data incident will have a measurable effect on the outcome. A data incident that could potentially cost millions of dollars and shatter an organization's reputation can, if handled effectively, be brought under control and have a significantly reduced impact. Following a well-publicized data breach involving malware installed on Home Depot's self-checkout kiosks, two Canadian firms launched class action lawsuits seeking \$500 million; the lawsuits ultimately settled for \$400,000. The significant reduction was warranted, said the judge, because of Home Depot's "exemplary" response to the breach:¹

"In the immediate case, given that:

- (a) Home Depot apparently did nothing wrong;
- (b) it responded in a responsible, prompt, generous, and exemplary fashion to the criminal acts perpetrated on it by the computer hackers;
- (c) Home Depot needed no behaviour management;
- (d) the Class Members' likelihood of success against Home Depot both on liability and on proof of any consequent damages was in the range of negligible to remote; and
- (e) the risk and expense of failure in the litigation were correspondingly substantial and proximate,

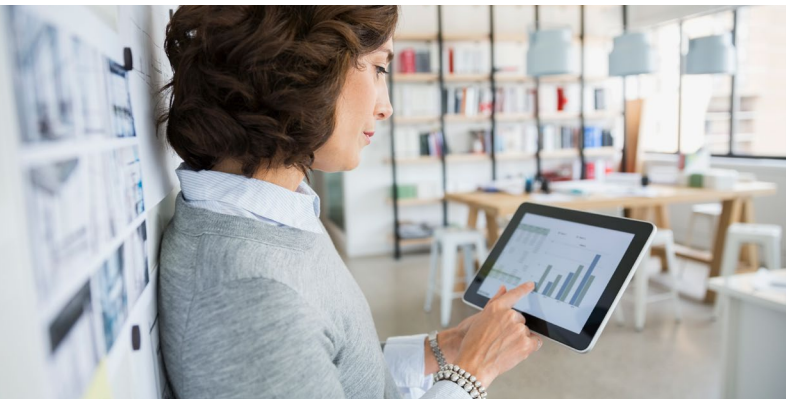
I would have approved a discontinuance of Mr. Lozanski's proposed class action with or without costs and without any benefits achieved by the putative Class Members."

More Data

Data about an identifiable individual constitutes personal information. As a result, the collection of this kind of data creates privacy obligations and triggers privacy laws.² With advances in technology, organizations are collecting, using, storing, and transferring more personal information about their consumers, professionals, patients, and employees than ever before. The accumulation of vast amounts of personal information in large databases increases both the risk and potential impact of unauthorized use or disclosure of that information. Moreover, recent technological innovations – such as in artificial intelligence – enable organizations to use data in new and powerful ways. As such, a single data incident involving personal information can now affect millions of individuals.

Larger and More Complex Data Incidents

Data incidents continue to grow in size and complexity. This reflects the increasing sophistication of the actors behind such incidents. The perpetrators' business models have evolved, and in addition to using more complex methods, their targets have shifted. The perpetrators' modus operandi has moved from stealing credit card information for unauthorized transactions to more malicious and damaging social engineering methods that allow access to a company's most valuable information. This information can then be monetized through insider trading, sale on the black market, or the demand of a ransom for its return.



Not If But When

Senior management's concern about a data incident has risen dramatically. It has become accepted wisdom that companies should not be asking if a data incident will occur, but when.

More Costly Data Incidents

Data incidents are becoming increasingly expensive. The cost of managing a data incident can be substantial. While new products, such as cybersecurity risk insurance, are available to help defray costs, litigation (especially class action litigation) is now a standard response to a report of a data incident. While damage awards have varied, organizations need to be prepared for the worst.



The costs do not end with damages – accountability for data incidents can reach into the boardroom. Senior executives frequently find themselves with their jobs on the line based on how they handle a data incident.

For example, Equifax's CEO Richard Smith resigned following criticism over the company's 2017 data breach.³ The chief information officer and chief security officer also stepped down.⁴

Finally, there are regulatory costs. Quebec's recently proposed change to its provincial privacy legislation includes administrative penalties of up to \$10 million or 2% of worldwide turnover, whichever is greater, and penal sanctions of up to \$25 million or 4% of worldwide turnover.⁵ Under Canada's

Personal Information Protection and Electronic Documents Act ("**PIPEDA**"), failure to comply with the mandatory breach notification requirements can result in fines of up to \$100,000 per violation.⁶ There are several privacy law reform efforts underway in Canada and the Privacy Commissioner of Canada has repeatedly called for the power to issue fines.⁷

From Compliance to Competitive Advantage

Previously viewed as an unwieldy compliance effort that saw little in the way of return on investment, savvy companies now see enhanced data protection and a robust incident response plan as a competitive advantage. Cybersecurity expenditures serve a strategic, profit-driving function. For example, a recent survey by Bain & Company found that customers would pay an average premium of 22% for better security and data practices.⁸ Further, Cisco's 2020 Data Privacy Benchmark Study, which surveyed respondents in 13 countries including Canada, found that more than 40% of organizations investing in privacy instruments are experiencing returns at least twice that of their privacy spend.⁹ Unlocking such premiums should be a key goal of any cybersecurity framework.



02

Why Cybersecurity Preparedness Matters

Better Outcomes

The first 72 hours are critical. While not all data incidents are of headline-grabbing magnitude, the worst incursion can throw an entire organization into turmoil for months. The first 72 hours after a data incident are, in particular, a chaotic mix of moving parts, most of which have to be addressed simultaneously, all while relying on information which is not yet complete.

A cybersecurity incident response plan that has been prepared in advance for implementation by a trained and tested incident response team goes a long way towards staving off potential chaos, keeping key players on-message, and focusing the efforts of the team on identified priorities. Importantly, an incident response plan lends structure to the urgent work and can represent an important brake on unfocused activity and the urge to “do something”. Moreover, a tightly-scripted response can reduce costs, reduce the over-involvement of outside vendors, help preserve evidence that may establish that the organization met the applicable standard of care, and minimize reputational damage.

This incident response plan should be part of the greater privacy management program that every organization handling personal information should put in place.¹⁰

Evolving Standard of Care

A properly designed, documented, and executed incident response plan is critical to limiting data loss and organizational disruption. More importantly, it may assist in reducing liability to third parties and regulators provided that the plan is regularly updated to reflect changes in cybersecurity awareness.



An organization, if sued, may ultimately have its incident response plan and its implementation of the plan evaluated by a court. A court charged with evaluating the reasonableness of an incident response plan will look not only at the paper documents that an organization relies on but, among other things, whether policies were followed, whether appropriate technical, financial, and employee resources were allocated, and whether senior management was involved in the creation and management of the plan. Further, with new risks and threats being identified every week, an incident response plan cannot be a static document.



The standard of care may also be evaluated against regulatory guidance in specific sectors. For instance, the Office of the Superintendent of Financial Institutions (“**OSFI**”) has stated that federally-regulated financial institutions (“**FRFIs**”) “must address technology and cybersecurity incidents in a timely and effective manner.”¹¹ OSFI requires incident reporting in order to identify steps to “proactively prevent such incidents” and improve resiliency.¹²

A proactive approach includes appropriate policies, staff, processes, practices, and technologies used to assess and mitigate cyber risks and attacks.

While OSFI does not explicitly require FRFIs to have an incident response plan, it has nonetheless recommended that such plans be drafted and maintained in order to adequately prepare for cyberattacks. Notably, in 2013, OSFI published a “Cyber Security Self-Assessment Guidance” memorandum, which provides that FRFIs should have in place an “Incident Management Framework [that] is designed to respond rapidly to material cybersecurity incidents”; “document[s] procedures for monitoring, analyzing and responding to cybersecurity incidents”, and that contains a “change management process [...] designed to allow for rapid response and mitigation to material cybersecurity incidents.”¹³

Similarly, the Canadian Securities Administration (“**CSA**”) does not explicitly require members to have an incident response plan in place. However, in an October 2017 notice, the CSA advised members to establish and maintain an incident response plan “to respond to and to escalate a cybersecurity incident.”¹⁴ The CSA further noted that this guidance would be considered “when assessing how firms comply with their obligation to manage risks associated with their business” during compliance reviews.¹⁵ The cybersecurity concerns and expectations of securities regulators, including the CSA, are addressed further by this guide, below at section IV(f).

Key Elements of a Framework



Governance



Training and
Policies Plan



Third Party Access
and IT Service
Agreements



Security, Malware
and Monitoring



Cybersecurity
Risk Insurance

03

Cybersecurity Preparedness and Incident Response Plan

While data incidents are occurring with increasing frequency, if properly managed, they need not be a catastrophe. Organizations that integrate incident preparedness and prevention into their overall cybersecurity risk management program are significantly more likely to have favourable outcomes in the event of an incident (and more likely to avoid an incident altogether) than organizations which adopt an ad hoc approach. In the context of a breach, a “more favourable outcome” includes an incident resolution process that:

- attracts limited media attention;
- minimizes costs (particularly costs associated with the threat of litigation);
- limits reputational impact;
- streamlines stakeholder involvement; and
- invites minimal scrutiny from regulators.

A **cybersecurity framework** is proactive. It contains a complete set of organizational resources, including policies, staff, processes, practices, and technologies used to assess and mitigate cyber risks and attacks.

A **cybersecurity incident response plan** is reactive. It represents an enterprise-wide undertaking that provides a protocol for the entire organization and assigns accountabilities and sets up metrics to track organizational efforts to resolve the incident. It includes a variety of specific elements and covers a wide range of disciplines. Importantly, it is comprehensive and detailed, consisting of more than check boxes and to-do lists.

Cybersecurity Framework

Governance

Cybersecurity is not solely an information technology risk. Rather, it is an enterprise-wide risk, and should be part of a board of directors’ general risk management mandate.

Cybersecurity needs to be addressed at the highest levels of the enterprise. Responsibility for cybersecurity, as with any critical business risk, ultimately falls to the board of directors. In the event of a data incident, courts will examine the involvement of directors in assessing and evaluating cybersecurity risks.

In the event of a lawsuit against directors and officers following a data incident, shareholders may challenge not only the directors’ and officers’ conduct in response to the data breach, but also allege that conduct following discovery of the data breach was improper.



Management and boards need to be proactive.

The following points represent important steps that should be considered by an organization's leadership when identifying and assessing an organization's cybersecurity risks.

Actions of Directors and Officers¹⁶

- Adopt written cybersecurity policies, procedures, and internal controls, including when and how to disclose an incident.
- Implement methods to detect the occurrence of a cybersecurity incident.
- Discuss at the management and board level the appointment of a chief information officer or a chief information security officer with the expertise to regularly meet with and advise the board of directors.
- Give consideration to appointing a board member with cybersecurity expertise and experience (or the board of directors should seek out an expert consultant who can provide advice to the board of directors), and to appointing an enterprise risk committee.
- Review annual budgets to ensure appropriate allowances for privacy and IT security programs.
- Receive regular reports on data incidents and cyber risks.
- Maintain a clear understanding of who in management has primary responsibility for cybersecurity risk oversight and for ensuring the adequacy of the company's cyber risk management practices.
- Give consideration to which risks are to be addressed and mitigated directly and which may be transferred through insurance.

Policies and Training



A key element of a cybersecurity risk management program is an organization's policies and procedures.

While the content of policies may vary, there are certain important common elements.

The specific components of any program will vary from organization to organization depending upon jurisdiction, industry, and an organization's risk tolerance. However, all policies should be written in plain language and be easily accessible (such as through the organization's intranet). All employees, regardless of their level or position, should be able to understand the policies and receive formal training on how best to comply with them.

Some specific areas for training and policies may include the following considerations:

IT Security

Does the organization have materials and training that provide guidance to the information security team? Items that such a policy might address include:

- Access control and password management.
- Network connection and firewall management.
- Virus and malware management, including installing updates and patches, and change control mechanisms.
- Encryption requirements.
- Network security, including wireless network security.
- Preparing for, recovering from, and responding to a data incident, including a mechanism for reporting of incidents.
- Remote access to the organization's networks.
- Disposal of IT assets, devices, and data (including a data retention policy).
- Business continuity and disaster recovery.

Acceptable Use of IT Assets

- Does the organization have plain language policies available to employees that set out the acceptable use of information systems and assets, email and other communications services, internet, devices, and so on?
- Does the organization's policy explain what will be an acceptable use of social media for business purposes, including social media posts in which the organization is identified?

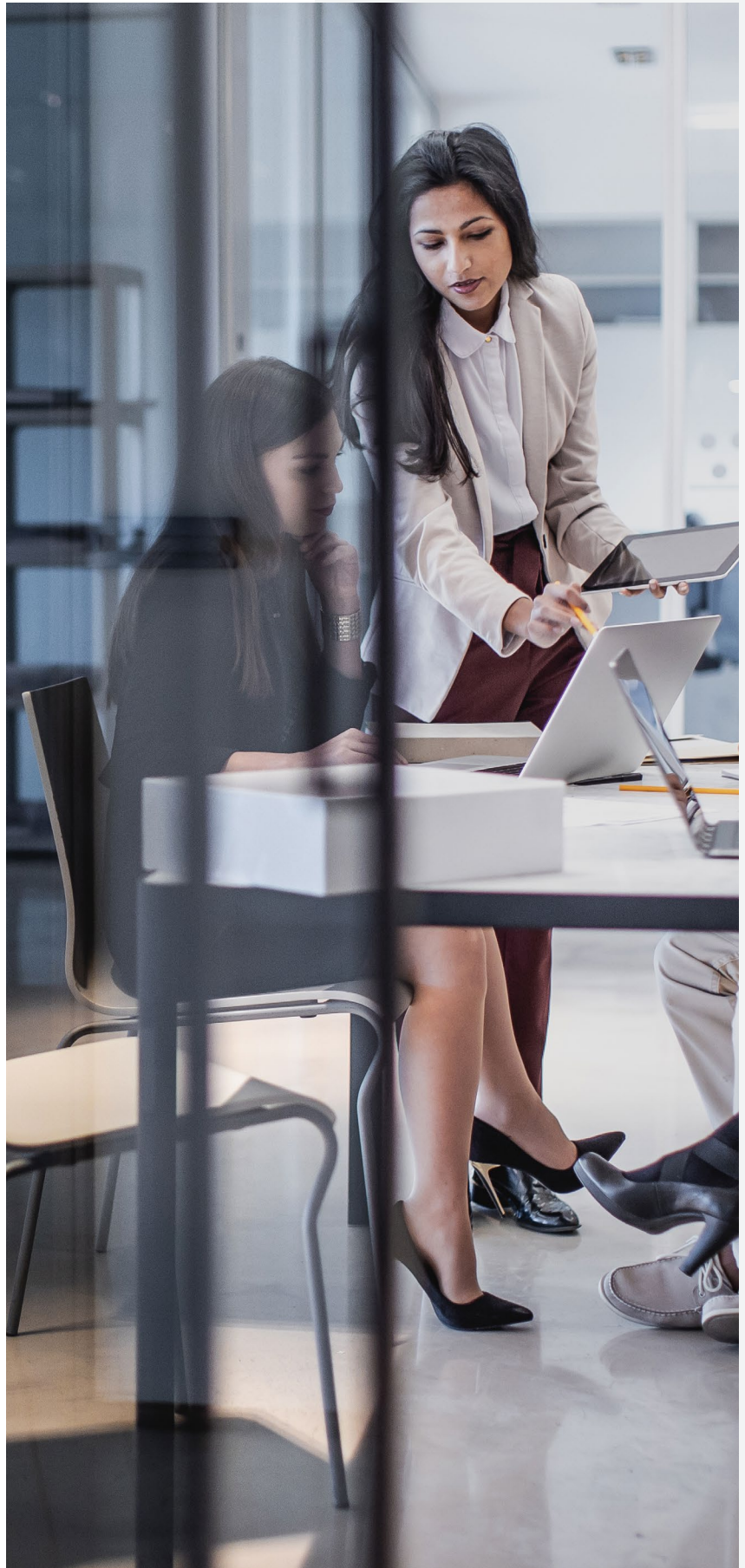
- Does the organization have a policy that addresses use of employee-owned devices (BYOD) for the organization's business?
- Does the organization have a policy that addresses employees working from home/home offices and the use of mobile devices and portable data storage (such as USB keys, portable hard drives, etc.?)

Employee Education and Training

- Does the organization have formal written policies and do employees receive regular training, with successful completion of such training documented?
- Is training done during onboarding, when the employee's role changes and on an ongoing basis and when there is a significant change to a policy?
- Is training documented and do employees sign off each time they successfully complete it?
- Do departing employees receive an outgoing interview to remind them of their ongoing obligations and to ensure information assets and devices are returned?

Vendor Due Diligence

- Does the organization have a policy that sets out what will constitute ordinary and sufficient due diligence for all vendors that will have access of any kind to the organization's IT system?
- For vendors that are actually supplying IT assets or services, due diligence in respect of negotiating and enforcing the cybersecurity terms in their contract will be important and is discussed in more detail in the sidebar Examples of Vendor Due Diligence Inquiries.



Examples of Vendor Due Diligence Inquiries

- What is the state of the vendor's security framework? What policies and procedures does it have in place to maintain the integrity of the framework?
- Will the vendor permit penetration testing and other exploration of vulnerabilities?
- Are the vendor's facilities audited for industry-recognized internal controls? Does the vendor perform internal audits, and is it willing to share the results with the client?
- Where are the vendor's service delivery centres? Where does it process and store data?
- What cybersecurity risk insurance does the vendor carry, and has it made any claims in the last five years?
- Is the vendor operating in accordance with industry-recognized security standards (including those related to cloud computing, if applicable)?

Third Party Access and IT Service Agreements

The most basic form of access control is user privileges, which refer to the rights a user has to access company systems and data. The prevailing principle is that of "least privileges", which dictates that users be granted only the level of access necessary for them to do their job.

The "least privileges" principle applies not only to employees, but also to vendors and other third parties. In many cases, these types of relationships will be governed by contracts, which can also become a key element of cybersecurity preparedness, with

provisions geared towards prevention, response, mitigation, and remedy.

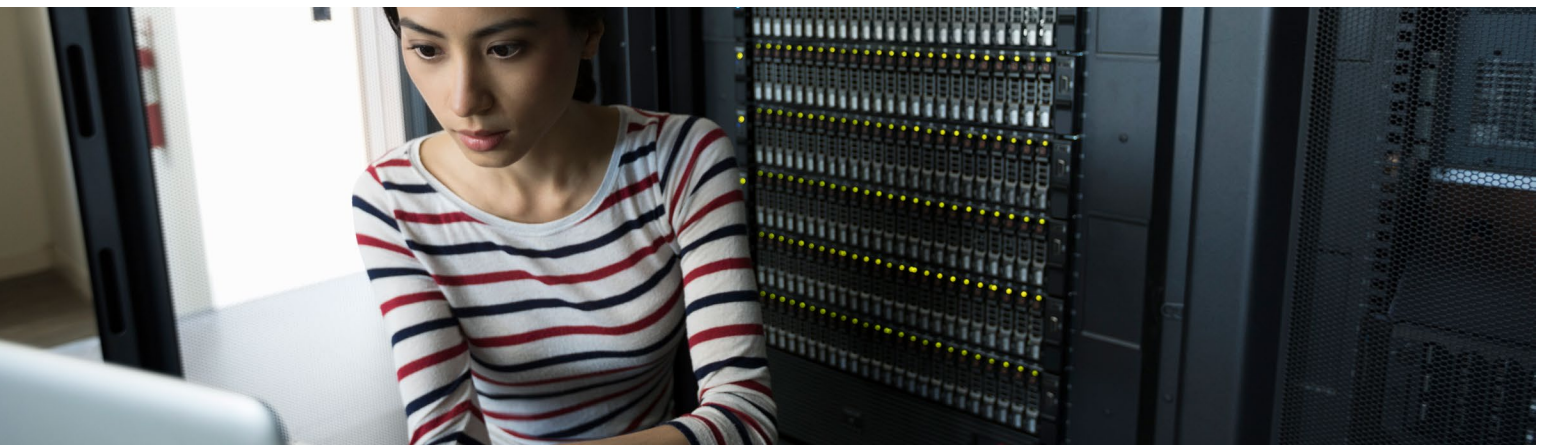
There are two general third party scenarios: the first is where an organization is contracting with a vendor for actual IT services, and the second is where an organization is contracting with a vendor for some other product or service which requires access to the IT system (such as a lighting services supplier who needs access to an organization's IT systems for environmental monitoring). While both scenarios require cybersecurity due diligence, the due diligence considerations go much deeper for the first scenario.



For an IT services agreement, the starting point will be to understand the organization's cybersecurity risks (see sidebar Examples of Factors in Evaluating an Organization's Cybersecurity Risk Profile).

In addition, conducting proper due diligence on a potential vendor is an essential part of getting a best of breed contract in place. The structure and components of the vendor's solution, and the vendor's capabilities and certifications, risk management practices, and financial wherewithal are all elements that should be explored.

Having established the organization's cybersecurity risk profile, and having completed thorough due diligence of the vendor, the legal team will then be in a position to tailor the various data incident prevention, response, mitigation, and remedy provisions of the proposed IT services agreement.



Some of the most important provisions in the agreement will pertain to risk allocation. The interplay of representations, warranties, indemnities, and liability is generally hotly contested in the area of cybersecurity as jurisprudence continues to evolve. An organization may want to consult outside legal counsel with expertise in this area to determine how it wishes to effectively address these issues and to discuss the various avenues available.

IT Security, Malware, and Monitoring

IT defences are critical to managing an organization's risk. These should be comprehensive, up to date, and tailored to current and anticipated threats. It is important for an organization to subscribe to a comprehensive and legitimate threat assessment service (for instance, Canadian Cyber Incident Response Centre (CCIRC) Cybersecurity Bulletins and best practice documents).¹⁷ There are also industry and public sector organizations that are engaged in information sharing. For instance, in 2019 the Bank of Canada announced a public-private partnership with the Canadian Financial Sector Resiliency Group to coordinate responses to sector-wide incidents and protect critical infrastructure.¹⁸

Industry-standard antivirus and malware protection should be installed, with updates continuously installed and documented. The organization's networks should be protected from internal and external attacks, and wireless networks should be secured using industry-standard practices. Firewalls and malware detection should be routine and penetration testing should be conducted regularly (ideally by an independent third party). There should be technical solutions in place that detect and block suspicious activities or access.

Social engineering attacks should also be considered. Organizations should train their employees on how to avoid falling victim to phishing attacks, evil twin routers (a rogue Wi-Fi access point that appears to be a legitimate one offered on the premises, but actually has been set up to eavesdrop on wireless communications whereby an attacker fools users into connecting a laptop or mobile phone to a tainted hotspot by posing as a legitimate provider), and USB keys that appear to have been lost but are deliberately-planted malware-infected devices.

Cybersecurity Risk Insurance

As data incidents increase in number, scope, and impact, organizations are looking to transfer the risk associated with them. The most common way of transferring risk is by obtaining insurance policies: if the risk is insurable, the risk is transferable. For example, Marsh Inc., a global insurance broker, estimated that the number of organizations that purchased cybersecurity risk insurance in the US increased from 19% in 2014 to 38% in 2018. This number will only increase in the years ahead as awareness of the high cost and prevalence of cyberattacks grow.¹⁹

Examples of Factors in Evaluating an Organization's Cybersecurity Risk Profile

- Is the organization in an industry with a regulatory framework that dictates certain cyber-protection measures? For instance, if an organization operates in the financial services industry in Canada, the agreement will have to comply with existing and emerging regulations and guidelines promulgated by OSFI, IIROC, and CSA.
- Does the organization do business in multiple jurisdictions? Where is it collecting, processing, and storing data?
- Is the organization a private company, or a public company with many shareholders and subject to exchange oversight?
- Will the organization be handling personal information? Does it include personal health information? If so, existing and evolving privacy protection laws will come into play.
- Will the IT solution be B2B or B2C?
- Will the IT solution involve third party interventions, such as hosting or payment providers?
- Is the organization storing its data onsite, in a local data centre, or in the cloud?



Generally, cybersecurity risk insurance is divided into first party coverage protecting the policyholder, and third party coverage for third party claims against the policyholder.

First party policies may cover costs and losses associated with:

- a)** Investigation and the process associated with determining the scope of the incident, the extent of the damage, and taking steps to stop the incident;
- b)** Providing notice to individuals whose identifying information was compromised or otherwise affected by an incident. Some policies may include coverage for credit monitoring services as well as establishing a call centre;
- c)** Public relations services to counteract the negative publicity that can be associated with a data investigation;
- d)** Responding to government investigations;
- e)** Replacing damaged hardware or software;
- f)** Responding to parties vandalizing the company's electronic data;
- g)** Business interruption, including in relation to any downtime, data loss, data recovery, and costs related to reputational damage; and
- h)** Lawsuits and extortion. An incident may result in legal expenses or could include costs related to cyber extortion, such as ransomware.

Third party policies may cover liability in respect of:

- a)** Permitting access to identifying information of customers;
- b)** Transmitting a computer virus or malware to a third-party customer or business partner;
- c)** Failing to notify a third party of their rights under the relevant regulations in the event of a data incident; and
- d)** Potential "advertising injury," including harms through the use of electronic media, such as unauthorized use or infringement of copyrighted material, as well as libel, slander, and defamation claims.

Cybersecurity risk insurance can also specifically cover the crisis stage of a data incident. This could include any expenses related to the management of the incident, such as investigation, remedial steps, required notifications, call center set-up and public relations management, credit checks for the subjects of the data, and any legal costs (including fines, or the costs of launching or defending a lawsuit).

Because all insurance policy coverage is dependent on the particular terms and conditions in the policy at issue, organizations looking to obtain cybersecurity risk insurance should consider a number of questions, and have their policies reviewed by legal counsel.

Examples of Cybersecurity Risk Insurance Considerations:

There is no standard policy an organization can obtain for cybersecurity insurance. In determining what kinds of coverage an insurance provider will include in a given cybersecurity risk policy, an insurer will consider, without limitation, the following factors:

- a)** Basic information about the organization, including its industry and the nature of its business;
- b)** The kinds of data collected and handled by the organization and the nature of sensitive information the organization deals with;
- c)** The organization's relationships with outsourcing providers and whether security, privacy, and risk assessments are performed internally or by third parties;

- d) A record of the organization's incident loss history and past security breaches and their impacts on the organization;
- e) The technological infrastructure of the applicant organization;
- f) The organization's policies currently in place to secure user access;
- g) The organization's current privacy policies and information and network security policies; and
- h) Technical measures incorporated by the organization to protect the information system.²⁰



In approaching and negotiating with a potential cybersecurity insurance provider, an organization should explore the following:

- a) What security controls can your organization put into place that will reduce the premium?
- b) Will your organization have to undertake a security risk review of some sort?
- c) Will your organization retain the right to choose its legal counsel in the event of litigation related to the incident?
- d) What is expected of your organization to reduce or limit the risks?
- e) Will your organization get a reduction for each year it does not make a claim against the policy?

- f) Could your organization claim if it was not able to detect an intrusion until several months or years have elapsed, finding itself outside the coverage period?
- g) Who makes the decision to pay/not pay ransom?

Cybersecurity Incident Response Plan

Until now, this guide has focused largely on the *proactive* elements of a cybersecurity framework. The other major part of cybersecurity preparedness is the *reactive* cybersecurity incident response plan.

An effective incident response plan ultimately relies on executive sponsorship. Developing an effective incident response plan requires ensuring that the right team is involved. An incident response plan should be enterprise-wide, and draw on the experience of key personnel from key stakeholder areas within the organization. Typically, this will include senior representatives from legal, public relations/marketing, customer care, human resources, corporate security/risk management, and IT. Ideally, it will also include pre-screened and pre-selected external advisors.

The responsibilities of the team and further details of the incident response plan are set out in the next section, **Part 4**.

Once the incident response plan is drafted, it should not sit in a drawer. Organizations should train, practice, and run simulated data incidents to develop response “muscle memory.” The best-prepared organizations routinely conduct war games to stress-test their plans, increasing managers’ awareness and fine-tuning their response capabilities. Outside legal counsel, with sophisticated understanding as a result of having handled dozens of data incidents, will often be invited to run the simulation, and evaluate the organization’s response.



It is also important to note that in the event of a ransomware attack, it may not be feasible to pull up a copy of the incident response plan stored electronically. Organizations should be prepared by having physical copies of the incident response plan available to key stakeholders.



The incident response plan should be comprehensive and address every phase of the cybersecurity incident. Its components should include, at minimum:

- 1.** A core internal team of decision makers, including executive leadership, legal, public relations/marketing, customer care, human resources, corporate security/risk management, and IT.
- 2.** External resources with retainers in place, specifically in respect of legal counsel and a forensic auditor. Outside legal counsel can advise on regulatory compliance obligations and assist with directing the response in preparation for potential litigation (including in regards to steps that should be taken to maintain legal privilege). Forensic auditors help determine the source and scope of an incident, which will in turn inform reporting and notice obligations. Where required, external legal and forensic service providers should be approved by the insurance provider in advance of an incident.
- 3.** An incident classification framework, with higher classifications triggering a more robust response.
- 4.** A data map that includes what sensitive information the organization has and where it is stored.
- 5.** A list of internal and external parties that need to be notified of an incident, which may include:
 - a) Third parties who have provided confidential/personal information to the organization and have a right at law or under contract to be notified of an incident;
 - b) Law enforcement;
 - c) Federal or provincial privacy commissioners that may have jurisdiction;
 - d) Insurer/insurance broker;
 - e) The Board of Directors; and
 - f) Customers and other affected individuals and stakeholders.
- 6.** An incident response log.
- 7.** An outline of next steps and processes for chronicling lessons learned.

04



What To Do When the Worst Happens: Executing the Cybersecurity Incident Response Plan

A cybersecurity incident response plan should be prepared in advance, detailed, tested, and well-understood by those within the organization responsible for its implementation. An incident response plan will focus the efforts of a diverse group of people during a crisis, and help prevent well-meaning but uncoordinated communications (both internally and externally).

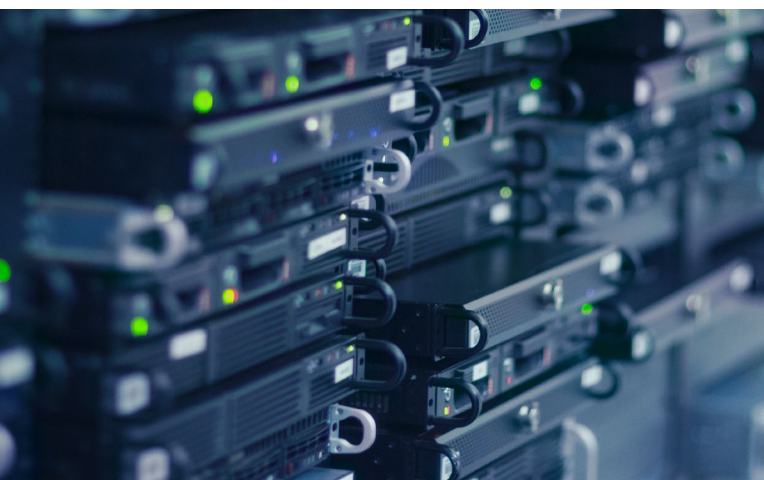
An incident response plan should be the result of input from stakeholders enterprise-wide. Each stakeholder will ultimately have to designate someone from their group to be their lead on the team, meaning they will be accountable for executing their portion of the plan as well as responsible for reporting to management.

Several steps are involved in any incident response plan:

Contain the Incident

Not every data incident will involve sophisticated hackers compromising an organization's IT systems. Physical incidents (such as non-electronic breaches such as departing employees taking information with them, loss of records or devices, break-ins, theft of laptops, etc.) are still common. Organizations should note that the incident response plan should not only contemplate activation in the case of an electronic breach, but in the case of a critical non-electronic one as well.

Depending on the scope and nature of the physical data incident, it may or may not be appropriate to activate the incident response plan and convene the incident response team. Regardless, the first step will be to promptly investigate and take action to limit further data loss. This can be done by limiting employee and public access to the affected area and changing locks/access cards if necessary. Organizations should determine whether it is appropriate to notify law enforcement. If an internal or external investigation is being conducted, the organization will need to determine what assets have been lost/affected, obtain tracking information (if available), obtain video surveillance (if available)



and, if the incident involved employee misconduct, consider HR implications of any such investigation.

If an electronic data incident has occurred (such as a hack or other compromise of IT infrastructure that has led to data loss or infiltration), containment is likely to be more challenging and it is more likely that an organization will need to implement its incident response plan and convene the incident response team. These decisions will largely turn on the size of the incident and the type of information affected.



Immediately After Discovery

Recording information about a breach is essential as recent amendments to PIPEDA require organizations to keep and maintain records of every breach of security safeguards involving personal information under their control, without regard to the gravity of the breach.

The discovery: Record the date, time, location and duration of the breach (such as was it a one-time incursion, or has the malware been resident for months?) Document who discovered the breach and how.

The breach: Document the details of the breach (such as point of entry, method of intrusion, systems affected, whether information was accessed, deleted/modified or taken).

The data: Document the details of the compromised data (such as who are the individuals affected? Where are the affected individuals located? What type of information was compromised? Was the information encrypted? How many records are affected?).

Where appropriate, immediately begin marking all written reports and other information generated as being “Privileged and Confidential: prepared at the direction of counsel in anticipation of litigation”.

Convene the Team

If appropriate, the various team members should be contacted and the team assembled and briefed

– communications may need to be by phone only (in some cases, new mobile phones) in order to prevent the use of a compromised email system and the risk of leaks. Secure communications, including secure phones, laptops, and networks, should also be made available to senior management and other critical employees.

Once the incident response plan is triggered, clear communication channels, reporting structures, and accountabilities should fall into place. When deciding on these channels and structures, it will be critical to have already considered the most efficient ways to include internal and external legal counsel in order to preserve privilege (where appropriate).

The actual members of the team will vary depending upon the organization and the nature of the incident. However, the responsibilities of team members will generally include the following areas.

Legal/Compliance will:

- Along with outside legal counsel, implement a privilege protocol;
- Determine if, when, and how to notify affected individuals, the media, law enforcement, government regulators, and other third parties (such as card issuers, banks, etc.);
- Have established relationships with outside legal counsel prior to an incident, and manage outside legal counsel during an incident response;
- Manage all statutory notifications in all jurisdictions and communications with privacy commissioners, regulators, and so on;
- Ensure internal documents and reports are generated at outside legal counsel’s direction;
- Issue and monitor a litigation hold;
- Control information and identify persons who are on the “need to know” list; and
- Review all outgoing communications, filings, reports, etc.

Public Relations/Marketing will:

- Be familiar with industry channels and players and will have identified key media strategies prior to an incident occurring;
- Have an internal communication plan to emphasize confidentiality, appropriate employee actions if media contact them, and a response plan if information about the incident is leaked; and
- Track and analyze media coverage and devise a plan to respond, if necessary, to negative coverage.

Customer Care will:

- Handle customer inquiries
- Create a rationale for determining whether incident inquiries will be dealt with internally or whether a call centre will be activated; and
- Where deemed appropriate, set up a call centre and consumer protection program (see below for more information, and Call Centre sidebar).

Human Resources will:

- Manage employees during the incident, including reallocation of employee resources as required; and
- Handle investigations, discipline, and termination if the incident is the result of employee wrongdoing.

Corporate Security/Risk Management will:

- Communicate with law enforcement (along with Legal), including RCMP, and possibly CSIS, CSE, the FBI and Secret Service – if the incident is of sufficient magnitude;
- Disseminate to the team any law enforcement directives and ensure compliance; and
- Manage incident risks, isolation of affected areas, and physical access.

IT will:

- Work alongside external IT forensics to identify and remove any malicious code or other artefacts of a data incident, if the source of the incident is electronic; and
- Assist with evidence, managing litigation holds, and supporting litigation efforts.



Analyse and Document the Incident

An organization should begin gathering relevant information the moment an incident is identified.

All information related to the data incident should be subject to a comprehensive litigation hold so that it can be preserved, collected, and analysed at the direction of legal counsel (and provided to law enforcement if required/appropriate). A subsequent review by lawyers will determine what information is actually relevant to any litigation and what information may be subject to legal privilege, but the first task will be to identify and preserve any information that might be relevant.

As the cause of the data incident becomes apparent, and affected individuals are identified, an organization will be in a position to predict how the compromised information might be used. Was it unencrypted personal financial information that was the subject of a malicious hack? Or was it the loss of an encrypted USB key with names and addresses only? The former is much more likely to end up being sold on the internet's black markets and used for fraud or identity theft. An organization can then begin making decisions about risk mitigation, consumer protection, and law enforcement.



When a data incident occurs, an organization will only have a short window of time to gather critical evidence



While the internal IT team will act as first responder to a data incident, they are often untrained in data recovery and forensic analysis and can sometimes do more harm than good by damaging critical data or inadvertently mishandling important evidence. For this reason, an outside IT forensics firm is likely to be one of the first outside vendors retained and operating after a data incident, using forensic software and protocols to perform data collection and data preservation in the wake of a data incident.

Where personal information is involved, organizations also need to create a record that is available for inspection by the OPC. For more details, organizations should review the OPC's website, which contains helpful guidance for businesses, updates, and frequently asked questions.²¹

Competencies of an IT Forensics Firm

The right IT forensics firm will:

- Be able to identify and neutralize the threat while at the same time preserving and handling evidence with proven, forensically sound methodology, using data recovery tools and processes that are supported by case law and prior litigation experience.
- Be able to work across operating systems, and across devices (not just computers, but laptops, handheld devices, GPS units, and in many cases, outdated technologies that are still in use).
- Be able to manage these critical steps in a way that respects employee sensitivities and workplace culture, because the firm will be interviewing and at least temporarily accessing employees' workstations and devices (and in some cases, personal devices).
- Be able to assemble a team with demonstrated experience supporting inside and outside legal counsel in building a case.
- Have key people who can provide testimony and appear as confident witnesses in court.
- Have a sophisticated understanding of privilege issues and litigation holds, be able to manage these issues, and understand the role that any and all of its investigations and reports may subsequently play in regulatory and court proceedings.

Organizations should have these relationships in place before an incident and, ideally, already have coordinated any anticipated response with their choice of external legal counsel in order to allow a seamless handoff of this critical phase during an actual incident response.

Assess and Manage the Legal Implications

At the same time as information is being collected and preserved, and as details of the nature and scope of the incident are just becoming clearer, the organization will also need to consider the medium- and long-term litigation risks arising from the incident. This step is frequently overlooked during the early stages of response to a data incident.

Litigation Risk – Class Actions

Privacy class actions are on the rise. Privacy class actions are generally brought (a) in the wake of a data breach, or (b) due to how a business collects or uses private information.

It is almost certain that, in the aftermath of any significant data incident, even arising from accidental or non-malicious disclosure, an organization will face at least one kind of class action. A consumer class action will almost certainly be brought on behalf of all customers potentially affected by exfiltration of personal information. If an organization is a Canadian public issuer whose share price dropped immediately after the announcement of the incident, an organization may be sued by a person representing shareholders, with an allegation that the organization's continuous public disclosure regarding the state of its cybersecurity systems was misleading.

Class actions may also be brought in reaction to companies' data collection, use, and disclosure practices. As customers and stakeholders increasingly claim to have a reasonable expectation that their data will be protected by the companies they transact with, claims have been commenced alleging that companies have (a) breached their privacy policy, (b) collected, used, or disclosed personal information without

obtaining proper consent²², or (c) disclosed personal information to third parties without first obtaining proper consent. While courts have often refused to certify such claims, as the collection of personal data grows, we can expect to see increased scrutiny by consumers and larger volumes of proposed class actions in this area in the future.

In Canada, a consumer or shareholder class action will almost always be brought in provincial (as opposed to federal) courts. Only one class action can proceed in each province and plaintiff law firms generally operate on the assumption that if they are the first to issue a claim in a particular province, that discourages competing lawsuits in the same jurisdiction. Accordingly, plaintiff law firms will generally issue a lawsuit in response to a data incident as soon as it can identify a suitable plaintiff who may have been affected. The statement of claim will likely have only generic wording, simply inserting the name of the organization and some basic facts about the incident. No investigation of the merits of a case will likely be undertaken before the proposed class action is issued (usually with an accompanying press release).

In an important decision rendered by the Superior Court of Quebec in the Equifax case,²³ the court ruled that the plaintiff had not presented sufficient evidence of damages to obtain authorization of a class action. The Court found the inconvenience of canceling credit cards and the psychological stress caused by knowing one's personal information was in the hands of ill-intentioned third parties constitute annoyances, fears and anxieties that everyone living in society must accept.

This decision constitutes a positive precedent for any company which, faced with computer fraud or a cyberattack, meets its obligations, in particular by notifying those affected. The simple fear that the personal information that is accessed in a breach will be used and the anxiety related to it are not necessarily sufficient to lead to the authorization of a class action, even in the presence of a finding of fault in the organization's security measures.

However, this statement must be qualified. This conclusion is not absolute. The decision of the Court could have been different if the applicant had had to incur costs to purchase identity

protection services or, again, if he had detailed the nature of the psychological or other damage he claimed to have suffered to show harm beyond what everyone living in society must accept.

For a class action commenced in a provincial court, the availability of common law and statutory causes of action will depend on the jurisdiction.

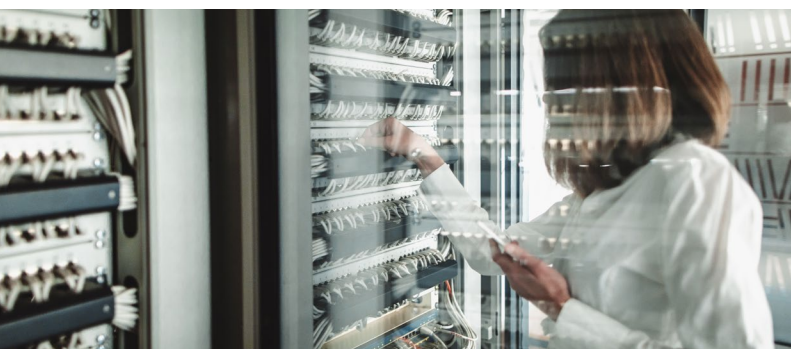
- Several provinces have statutory privacy torts. For example, British Columbia's provincial *Privacy Act* creates a statutory tort of intentional breach of privacy if a person, wilfully and without a claim of right, violates the privacy of another. This tort is actionable without proof of compensable damage. As a consequence of this statutory right, it is well-established in British Columbia that there is no freestanding common law tort of breach of privacy. Accordingly, if raised, such common law claims can be struck.²⁴
- By contrast, in Ontario, the Court of Appeal confirmed in *Jones v. Tsige* that there is a common-law tort of breach of privacy that applies to general personal information.²⁵ The court identified the basis for this new cause of action to be an "intrusion upon seclusion" based upon whether the defendant's conduct was: (1) intentional, (2) an invasion of private affairs without lawful justification, and (3) whether a reasonable person would regard the conduct as highly offensive/a cause for distress. The possibility that an organization could be liable under the tort of "intrusion upon seclusion" following a data breach was more recently supported by the Ontario Superior Court's decision in *Agnew-Americanano v. Equifax Canada*.²⁶ The case law relating to intrusion upon seclusion continues to evolve, with class counsel frequently pleading the tort in data-related actions.



- PIPEDA includes a private cause of action that can be brought by a complainant if the complaint results in a report or is discontinued by the OPB. It is presently not clear if a class action could be brought under this cause of action.²⁷
- Other privacy-related class action claims that have been brought on the basis of common law causes of action include the torts of negligence, breach of fiduciary duty, breach of confidence, breach of contractual terms governing the collection, retention and disclosure of personal information (including where there is a contractual commitment to comply with laws, which could include privacy statutes), and the failure to warn clients and customers after a privacy breach has occurred.

It is possible in Canada for overlapping class actions to be brought in multiple provinces; as a result, an organization may need to defend multiple parallel cases at the same time.

Whether one case or many, class actions tend to unfold slowly (especially where the facts are still being discovered and the law as to liability and damages is, as here, uncertain). It may be three to five years before a class action reaches trial or settlement. It is for this reason that an organization should include an outside litigation specialist on the incident response team, and involve them as soon as possible following an incident. It will be outside legal counsel who have their eye on the longer term consequences (asserting privilege, reviewing public messaging, and so on), while the organization and its resources are focused on the immediate response.





Regulatory Risk

An organization can also expect to be the focus of regulatory proceedings – principally meaning investigations by various privacy commissioners responding to complaints or acting of their own accord and, depending on the industry, also securities, financial institution or public health regulators, and even law enforcement agencies.

The main regulators in this area will be the various provincial privacy commissioners, as well as the federal commissioner. A chief concern for an organization that has suffered a data incident where personal information was involved will be providing notifications to the various privacy commissioners. See **Prepare and Send Reports to Commissioners and Notices to Affected Individual**, below, for a discussion of reporting to the relevant privacy commissioners.

Insurance Coverage

Does the organization have cybersecurity risk insurance? If so, is the incident covered and to what extent? Agreements and policies will need to be reviewed to make these determinations. As well, insurance agreements generally have a requirement that the insured promptly notify the insurer of a suspected incident. As part of an organization's cybersecurity framework and incident response plan, they will want to make sure they know when such an obligation is triggered, how long they have to report the suspected breach, and what information they are required to provide to their insurer.

Once the above is complete, the insurer should be notified, but only once legal counsel has been involved and approves the notification. For further discussion of cybersecurity risk insurance and what it may cover, see the discussion above at **Cybersecurity Risk Insurance**.

An insurer may be able to impose their choice of legal counsel or forensic auditor should a breach occur. To avoid such imposition, it is important that the organization discuss such decisions at the outset of a relationship with a given insurance provider.

Indemnification (by and responsibility of third parties or employees)

Where a third party (such as an IT service provider) is implicated in a loss of data, relevant agreements should be reviewed for indemnification clauses and any notification or informational requirements therein. Once the above assessment is complete, the third party service provider should be notified if appropriate, but only once legal counsel has been involved and approves the notification.

Employee liability and responsibility may also be in issue. A review should be conducted to determine if corporate policies were followed or if laws were violated, and appropriate, responsive actions should be taken. If the organization has a unionized environment, labour considerations may also be in play.



Criminal Code Offences

Identity theft and identity fraud

(ss. 402.2 and 403)

Identity theft is the possession and trafficking of information about another person's identity where the information will be used in certain listed crimes of deceit (forgery, fraud etc.). Identity fraud involves impersonating another person for the gain of the impersonator or to the detriment of the victim.

Unauthorized use of a computer

(s. 342.1)

It is an offence to fraudulently access a computer or data storage system belonging to someone else to download information or intercept private communications (such as a disgruntled former employee hacking into an organization's IT system).

Mischief to data (s. 430(1.1))

This offence criminalizes the unauthorized use of data that renders it less useful to its proper owner. Note that theft of confidential information is not caught by this offence and is difficult to place under any other existing Criminal Code offence because the Supreme Court of Canada has held that confidential information was not "property".

Unlawful interception of private communication (s. 184)

Intercepting or accessing a private communication is unlawful where the individuals have a reasonable expectation of privacy.

Terrorism (ss. 83.01-83.21)

Large-scale hacking that is designed to endanger the lives and safety of the public, or to disrupt an essential service, for a political, religious or ideological purpose may fall under this provision. It is an offence to participate in, facilitate, or instruct others to carry out this hacking activity.

Law Enforcement

Law enforcement may become involved. Such involvement can occur in two ways, either by law enforcement approaching the organization with a request for information or by the organization itself requesting that law enforcement become involved.

Organizations should be aware of disclosure restrictions. If approached by law enforcement, an organization should be aware that, depending on the jurisdiction, it may only be entitled to disclose personal information to law enforcement without the consent of the affected individual where it is required to do so pursuant to a warrant or summons, or as otherwise required by law.

Whether and when an organization may disclose personal information requested by law enforcement, but not required by law, is a complex and evolving area.

Law enforcement may also be involved because the organization has concluded it is the victim of a criminal offence (see sidebar Criminal Code Offences).

Once law enforcement is involved, they may request that breach notifications and other disclosures be delayed in order to preserve the integrity of their investigation, or they may otherwise prohibit the release of certain information. This may conflict with the organization's existing statutory or contractual obligations and, accordingly, legal counsel should be involved in all discussions with law enforcement.

Consumer/Customer Response

One of the most significant stakeholder groups in a data incident is an organization's customers. Canadian consumers have high expectations that not only will they be promptly notified about a data incident, but that organizations will take immediate, clear steps to protect consumers (or allow consumers to take steps to protect themselves). Further, an organization may be required to notify the affected individuals, as further discussed below at **Prepare and Send Reports to Commissioners and Notices to Affected Individuals**. The gap between what organizations do, and what consumers expect them to do, creates an area of risk.

Among other things, organizations should consider establishing a call centre to address consumer concerns. In addition, consumers often expect organizations involved in significant data incidents involving payment cards or identifying information to offer credit monitoring and identity theft monitoring.



A well thought-out and robust customer response can, in addition to helping retain customers and preserve brand value, have a significant impact on potential class actions fees and damages.²⁷

Call Centres

In the case of most large data breaches, a decision will be made to activate a call centre (as opposed to dealing with customers using internal resources on an ad hoc basis). The sooner a call centre is up and running, the sooner an organization can begin managing the message, limiting reputational risk, and attempting to curb the prospect of a class action.

Call centre considerations

- Can the service provider ensure the organization will be assigned a unique toll-free number for its customers?
- Will the number be truly toll-free and work in all affected jurisdictions?
- Can the service provider offer this service on a 24/7 basis?
- How long does the organization anticipate the call centre will remain active – and if that is unknown, can the activation period be open-ended?
- Is enrollment for protection products straightforward and easy to understand? Organizations will need to think about how to qualify callers for these products; in most cases, companies will want to have a low (or no) threshold to avoid further customer dissatisfaction.
- Does the service provider have sample scripts and FAQs that can be customized by an organization?
- Does the service provider have proficiency in both French and English? Other languages?



- All materials should be reviewed by legal counsel to ensure consistency of message and language. How quickly can legal counsel review and approve these scripts and FAQs?
- Is there a straightforward process for customers to sign-up for protection products?
- Does the organization have final say on all scripts? Or will the service provider insert its own language, and possibly use the opportunity to pitch to customers?
- Is there escalation to a fraud resolution specialist where appropriate?
- Can the service provider provide tracking and reporting services? Organizations will need this information to monitor the progress of their data incident resolution efforts. Factors like daily call volume, type of calls, speed of answer, and other metrics should be considered.

Protection Products

There are typically two main types of protection products that are offered: credit protection and identity theft protection.



Credit protection involves no-cost credit monitoring for customers and alerts customers if there is activity or something new on a customer's credit report.



Identity theft protection involves monitoring a customer's driver's licence, social insurance number and other foundational identity documents and online activity to see if any personal information is being bought or sold online, and monitoring court records and other markers of possible identity fraud.

These protection products may not be required in all cases. An organization affected by a data incident will need to consider carefully what products it will offer and, if it decides not to offer certain products, understand that the decision will come under significant scrutiny, particularly if it later emerges that such protection may have been warranted. The provision of such services also assists in mitigating possible damage, which will be a factor in any subsequent litigation.

There may be significant differences in the protection products that are available in Canada and other jurisdictions such as the United States. Where a data incident affects both jurisdictions, companies should expect to receive complaints or inquiries as to why better/longer/more complete services are being offered in one jurisdiction as opposed to another. These inquiries can be reduced if the organization's public statements mention only the fact that such products are being made available, but do not detail the nature of the products being provided in each jurisdiction.

Compensation

In some cases, fraud protection or identity theft monitoring may not be appropriate or feasible. In other cases, consumer goodwill may be at stake. In such circumstances, an organization may want to consider compensation. Ideally, this will have been explored well in advance of any data incident, and an organization will have a clear understanding of the form of such compensation, its distribution, the appropriate amount, and so on (such as gift cards to all consumers who present evidence of a purchase between qualifying dates). The compensation considerations should be documented in the organization's incident response plan.

Prepare and Send Reports to Commissioners and Notices to Affected Individuals

Notification to Privacy Commissioner(s)

As a practical matter, an organization may want to notify all relevant privacy commissioners when a breach occurs by using an approach that ensures a coordinated notification process that maintains consistency of information. Organizations must be aware that while information provided to a privacy commissioner will generally be confidential, some of it may be subsequently disclosed pursuant to requests made under access to information laws. There are now mandatory breach notification requirements (to both affected persons and the relevant privacy commissioner) under a number of privacy laws across Canada, including PIPEDA, Alberta's PIPA, and Quebec's recently proposed legislation (Bill 64, *An Act to Modernize Legislative Provisions Respecting the Protection of Personal Information*, which received first reading on June 12, 2020).

Organizations are obliged to notify both affected individuals and the OPC following a data breach when certain conditions are met. Among these conditions, an organization must report in writing to the OPC any **"breach of security safeguards"** involving personal information under its control if it is reasonable in the circumstances to believe that the breach creates a **"real risk of significant harm" to an individual** (or a **"RROSH"**). A breach of security safeguards is broadly defined in PIPEDA as: "the loss of, unauthorized access to or unauthorized disclosure of personal information resulting from a breach of an organization's security safeguards" or "from a failure to establish those safeguards."²⁹

PIPEDA defines a RROSH expansively and includes, among other things, "bodily harm, humiliation, damage to reputation or relationships, loss of employment, business or professional opportunities, financial loss, identity theft, negative effects on the credit record and damage to or loss of property". This expansive definition of harm imposes several new legal burdens on organizations.

The report of the breach must be made "as soon as feasible after the organization determines that the breach has occurred".



PIPEDA Breach Report Form for the Commissioner

Organizations that have noticed a breach creating a real risk of significant harm (RROSH) need to report to the OPC.

The report form should include:

- a) Information of a point of contact within the organization.
- b) Approximation of the number of individuals affected.
- c) Time of the breach and its circumstances.
- d) Description of the security safeguards in place at the time of the breach and of the personal information involved.
- e) Steps taken to notify affected individuals and mitigation strategy.

Further, an organization encountering a breach will have additional reporting obligations to other organizations and government institutions if the breached organization believes the other organizations may be able to reduce their risk of harm as a result.

These expansive mandatory breach obligations make it imperative that an organization engage external legal counsel as soon as a breach is detected in order to comfortably meet PIPEDA's "as soon as feasible" requirement. Non-compliance may result in the stiff penalties discussed below.

Penalties: An organization may be liable for fines up to CA\$100,000 per violation for knowingly violating the notification requirements. In early 2019, Innovation, Science and Economic Development Canada noted that "the threat of financial penalties causes organizations to pay attention" and called on Parliament to go beyond PIPEDA's current provisions

and to “strengthen Canada’s privacy framework”. It remains highly possible that subsequent legislative changes could lead to tougher enforcement and heavier fines.

Confidentiality: PIPEDA provides the Commissioner with the right to make public any information that comes to his or her attention in the performance or exercise of any of his or her duties, as well as information in security breach notification reports to the OPC, if he or she judges there to be a public interest for doing so.³⁰ This goes beyond the power to “name and shame” wrongdoers that the OPC already had under the previous PIPEDA regime.

Taken together, these provisions introduce more stringent privacy, consent, and breach notification obligations on organizations. Organizations must continue to balance these new obligations with the need to minimize financial and reputational costs stemming from a data breach. The changes introduced by the *Digital Privacy Act* have made the balancing act more complicated, made non-compliance more costly, and made a well-thought out incident response plan even more necessary.

Complaints from individuals to a privacy commissioner will trigger discrete investigations aimed at resolving the matter in issue, but privacy commissioners may also initiate an investigation of their own accord into any issue within their jurisdiction. Such investigations are more likely where there are multiple individual complaints, where the scope of the data incident is large or involves particularly sensitive information, where there is a larger public policy issue or need for guidance (such as a new type of service or business model), or where the relevant privacy commissioner feels that consumer or public interests have not been adequately protected by the organization’s response.



Notice to Affected Individuals



Where there is a real risk of significant harm, the organization must also notify the affected individuals. The notice must be “given as soon as feasible after the organization determines that the breach has occurred.”

The notification needs to be **conspicuous** and contain sufficient information to help affected individuals mitigate the risk of harm. Notifications sent to affected individuals must meet form and content requirements set out by section 10.1 of PIPEDA as well as by the *Breach of Security Safeguards Regulations*. More specifically, organizations must notify individuals of any breach involving their personal information that poses a RROSH as soon as is feasible. A notification must contain sufficient information to ensure the individual understands the risks posed by the breach, and what steps, if any, he or she can personally take to reduce or mitigate the harm. Such notification must include:

- A description of the circumstances of the breach;
- The date on which, or period during which, the breach occurred (or, if unknown, the approximate period);
- A description of the personal information that is the subject of the breach (to the extent that it is known);
- A description of the steps that the organization has taken to reduce the risk of harm that could result from the breach;
- A description of the steps that affected individuals could take to reduce the risk of harm that could result from the breach or to mitigate that harm; and
- Contact information that the affected individual can use to obtain further information about the breach.

Ensuring an individual receives a data breach notification that is understandable will allow them to identify risks and take steps to protect themselves from such risks if necessary. Where direct notification to affected individuals is not feasible, indirect notification (via newspaper ads, online or other notices) may be necessary.

Record Keeping Obligations

Under PIPEDA, organizations are required to “maintain a record of every breach of security safeguards involving personal information under its control”, irrespective of the scope of the breach or the sensitivity of the personal information involved.³¹ A “breach of security safeguards” means any “loss of, unauthorized access to or unauthorized disclosure of personal information” resulting from a breach of security safeguards or failure to establish security safeguards.³² The record keeping obligation is triggered by any breach, even if the organization determines that there is no **RROSH** arising from the breach. However, a RROSH triggers the obligation to report to the OPC and to notify affected individuals and, potentially, certain third parties.

Organizations are also required to “provide the Commissioner with access to, or a copy of, a record” on request.³³ The record retention period is two years and the record must include “any information that enables the Commissioner to verify compliance” with the mandatory breach notification provisions of PIPEDA.³⁴ Knowingly contravening the mandatory breach notification provisions is an offence that carries a penalty of up to \$100,000. The record keeping requirement is particularly important because the OPC has indicated that it will be conducting breach record inspections on a sector-by-sector basis.

How to Prepare Breach Record Inspections

To prepare for breach record inspections, we recommend organizations take the following steps:

- 1.** Verify that your organization is keeping records of each actual or potential breach of security safeguards, including:
 - a) Records that contain everything you must include in a report to the Commissioner had your organization reported the breach (as set out in the **Breach of Security Safeguard Regulations**); and
 - b) Your framework for assessing whether a breach of security safeguards results in a real risk of significant harm to the affected individual, including your basis for determining why **it was not necessary to report the breach (that is, on what basis you concluded that, in the circumstances you did not believe that the breach created a real risk of significant harm to the affected individual)**.
- 2.** Audit your breach records to verify that they include all of the information that is required by the **Breach of Security Safeguard Regulations**.
- 3.** Consider how many potential breaches of security safeguards that your privacy/legal/compliance departments have investigated. If the number is low, or zero, investigate if breaches are going unreported. Common breaches include lost or stolen devices (phones, laptops, hard drives, etc.), misdirected emails, and phishing attempts. One challenge with breach notifications is that employees do not always know that they must report the breach. Another challenge is that many security teams treat breaches of security safeguards simply as a security issue and fail to escalate the matter to legal or the other members of a multi-disciplinary incident response team. Accordingly, it is critically important that your incident response plan include proper employee training and clear incident response and escalation guidelines.



Meet Specific Industry Requirements

Certain industries have specific requirements for maintaining personal information and providing notification for a data breach. When developing a cybersecurity program, it is important to consider whether your business is affected by industry-specific privacy regulations.

International Considerations

Data incidents frequently cross international borders. As a result, organizations need to be aware of different requirements across jurisdictions. It is very important that outside legal counsel be involved in crafting an integrated response, as making disclosures in one jurisdiction may have consequences in others.

For example, organizations that process personal data of data subjects that reside in the European Union (“EU”), regardless of where the organizations themselves are headquartered or located, must comply with the EU’s *General Data Protection Regulation* (“**GDPR**”). The GDPR has rendered breach notifications mandatory in all EU member states where a data breach is likely to “result in a risk for the rights and freedoms of individuals”. Under article 33(1) of GDPR, organizations must notify³⁵ the supervisory authority³⁶ within 72 hours of first having become aware of the breach. Data processors are also required to notify the controller(s)³⁷ “without undue delay” after first becoming aware of a data breach. According to article 34(1), the controller(s) must communicate the data breach to the data subjects without undue delay where the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons.³⁸ The GDPR provides severe repercussions for organizations in breach of its requirements, including fines up to 4% of annual global turnover or €20 million (whichever is greater).³⁹

The United States has a patchwork quilt of data protection legislation that affects what organizations need to do in the event of a data incident. In 2018, the *California Consumer Privacy Act* (“**CCPA**”) was introduced as one of the most stringent data protection regimes in the United States. The CCPA affords California residents an array of data rights,⁴⁰ as well as a private right of action dealing with cybersecurity and data protection in certain circumstances.⁴¹

Healthcare

Personal information related to healthcare is generally covered by provincial laws. PIPEDA may only apply in certain situations, such as when a hospital is engaged in commercial activity beyond its core activities.

Alberta has mandatory breach notification requirements in its *Health Information Act*.⁴² Moreover, Ontario, Newfoundland and Labrador, New Brunswick, and Nova Scotia have privacy legislation which has been deemed “substantially similar” to PIPEDA with respect to health information custodians. For example, Ontario is governed by the *Personal Health Information Protection Act* (PHIPA), under which Ontario’s Information and Privacy Commissioner has issued health sector specific guidance for how to handle a data breach.⁴³

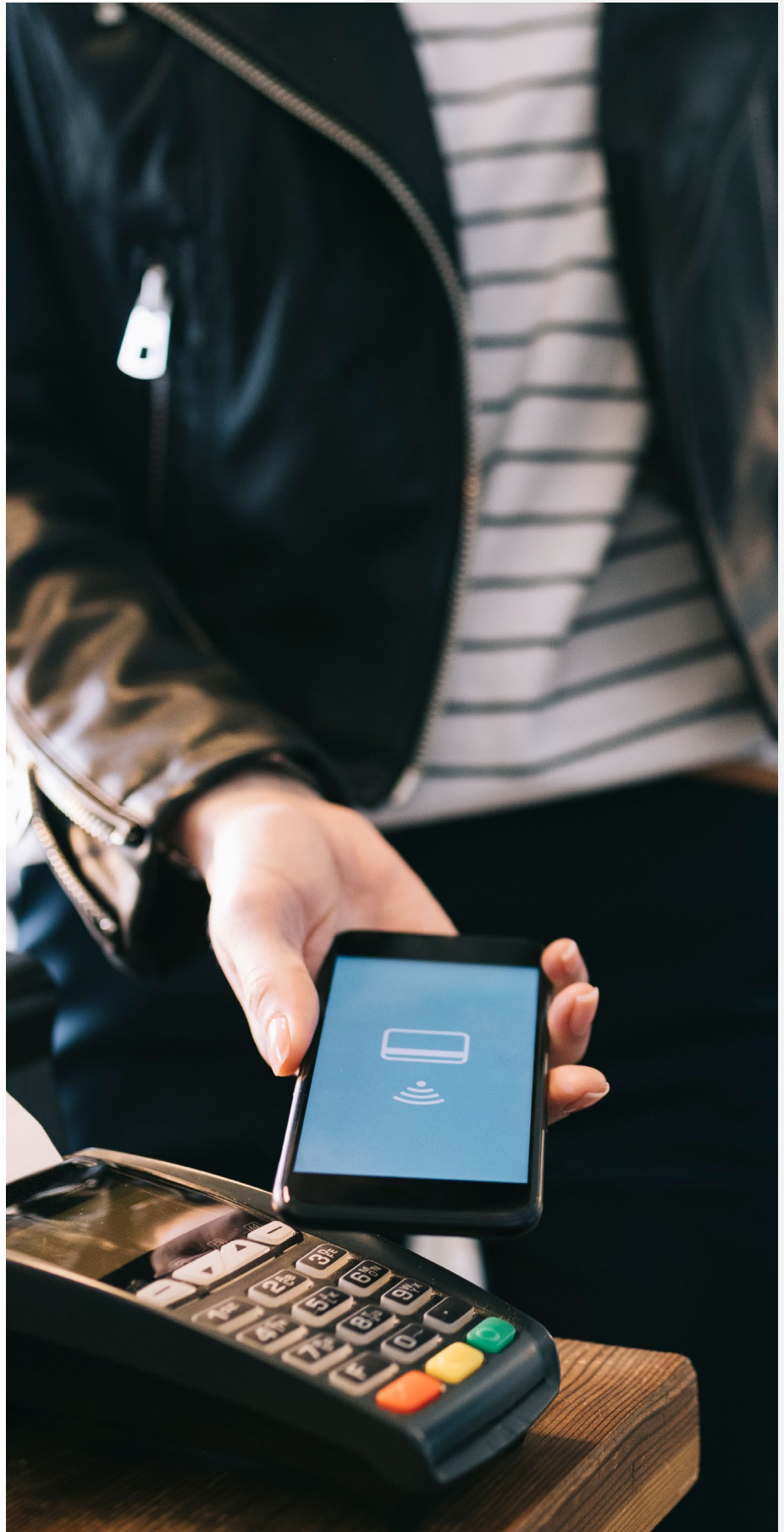
Payment Cards

Data incidents involving payment cards or the loss or unauthorized access to cardholder information raise special considerations in respect of the complex web of players in the chain of payment processors and the various contractual interrelationships. While there is currently no legislative or regulatory obligation in Canada to notify payment card providers or acquiring banks of a data incident, such obligations may well arise as a result of the various contractual relationships between (and among) the merchant organization and the various bank and payment card brands in respect of the use and issuance of payment cards.

There may be a requirement to comply with sector-specific standards. The Payment Card Industry Security Standards Council was founded by leading payment card brands. Organizations accepting payment card transactions – including acquirers, service providers, and merchants – from any of these payment brands have to comply with

the Payment Card Industry Data Security Standard (“**PCI-DSS**”) requirements.⁴⁴ Although the Security Standards Council has exclusive authority to set requirements, it does not participate in compliance enforcement. The card brands themselves are responsible for enforcing compliance for all transactions conducted with their own cards.⁴⁵ They accomplish this through policy enforcement with their member banks (acquirers). The member banks, in turn, enforce compliance with merchants. Consequently, if an organization wishes to process major credit cards, it must do so through members of the card brands, who mandate PCI-DSS compliance measures in their service contracts.

PCI-DSS requires documentation to be developed and maintained, preventive and detective security controls to be implemented, and processes to be in place in order to identify and contain any security breach attempts as soon as possible. A PCI-DSS Forensic Investigator (“**PFI**”), an IT forensics firm approved as a Qualified Security Assessor by the card brands, will conduct periodic reviews of an organization’s compliance with the PCI-DSS standards and issue reports that will recommend or decline continued certification.⁴⁶ Non-compliant organizations are subject to higher transaction fees imposed by their acquirer banks, contractual “penalties” imposed by the payment card brands, higher liability if a data incident occurs, and could run the risk of losing the authorization to process payment card transactions.



Additional, multiple sector-specific notifications may be required. When a data incident occurs, the compromised organization will often be required (in accordance with applicable payment card industry rules and requirements of acquirers, issuers and participating payment card brands) to notify their acquiring banks and participating payment brands, and may be contractually required to engage an approved PFI to investigate the security issue, determine the root cause, and report back to affected participating payment brands and others. The PFI investigation will often be conducted alongside the organization's own forensic IT investigation.



PCI-DSS does not provide specific guidelines on how to handle a security breach. Each payment card brand has its own policies and procedures, and they can differ among the individual brands. For example, some card brands require "immediate" notification upon confirmation of a data incident, while others require notification within 24 hours of knowledge of such incident.

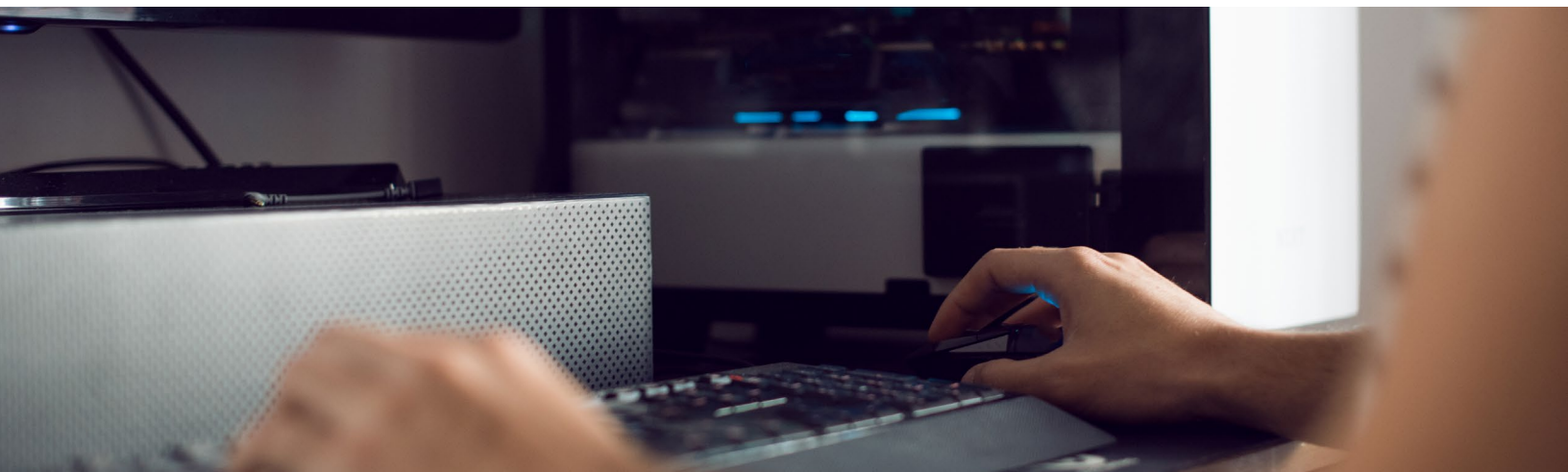
Some organizations may be tempted to defer or decline such reporting. However, even if organizations do not notify the bank and card brand network, it is very likely that these entities will independently identify the organization as a source of cardholder data compromise. Both banks and payment card networks have implemented processes to identify the source of an incident as precisely as possible.

Legal counsel should be involved in all discussions with PFI investigators and related investigations.

An organization may want to consult outside legal counsel with expertise in this area to determine how it wishes to manage not only the PFI investigation, but its interactions with card brands, the management of its own parallel IT forensics investigation, and the preservation of privilege. This is a complex, high stakes area and the strategic management of privilege issues will be of significant benefit to the organization.

Public Companies

Cybersecurity is a key concern of securities regulators. In October 2018, the United States' Securities and Exchange Commission ("**SEC**") released an investigative report that directed public companies to consider cyber threats when implementing internal accounting controls. The impetus behind the investigation and subsequent report was that nine public companies had recently been victims of fraud in the form of "business email compromises", where criminal perpetrators pretended to be company executives or vendors as a guise to receive large sums of money from unsuspecting recipients. Each company lost at least \$1 million dollars, while one lost more than \$45 million. SEC Chairman Jay Clayton said: "Cyber frauds are a pervasive, significant, and growing threat to all companies, including our public companies. Investors rely on public issuers to put in place, monitor, and update internal accounting controls that appropriately address these threats."⁴⁷





On March 1, 2019, the New York State Department of Financial Services (“**DFS**”) new cybersecurity regulation (the “**DFS Regulation**”) came into full effect. The DFS Regulation applies to banks, insurance companies, and other financial services institutions regulated by the DFS. The DFS Regulation is intended to protect both the information technology systems of regulated entities and the non-public customer information they hold from the growing threat of cyberattack and cyber-infiltration. Among other things, the DFS Regulation requires action in four key areas: (a) establishing a cybersecurity program; (b) establishing a cybersecurity policy; (c) designating a Chief Information Security Officer; and (d) reporting and records requirements. The DFS also recently announced the creation of a dedicated Cybersecurity Division, which will focus on protecting consumers and industries from pervasive cyber threats.

Public companies may be required to disclose risks in a number of disclosure documents mandated by United States Securities laws, despite no explicit obligation required by the public company. A public company should consider the materiality of such risks when preparing disclosure that is required under the *Securities Act of 1933* (“**Securities Act**”) and the *Securities Exchange Act of 1934* (“**Exchange Act**”). Such reporting obligations may include obligations within periodic reports, *Securities Act and Exchange Act* obligations, current reports and disclosure obligations related to risk factors.

The SEC has also stated that public companies should have policies and procedures in place that will assist to: “(1) guard against directors, officers, and other corporate insiders taking advantage of the period between the company’s discovery of a cybersecurity incident and public disclosure of the incident to trade on material non-public information about the incident, and (2) help ensure that the company makes timely disclosure of any related material non-public information.”⁴⁸

Under Canadian Securities Laws reporting issuers are required to disclose risks in a number of disclosure documents mandated by securities laws, including in prospectuses and in continuous disclosure documents such as annual information forms. For instance, the instructions to Form 51-102F1 (Management’s Discussion & Analysis) of National Instrument 51-102 (Continuous Disclosure Obligations) include a discussion of risks that have affected the financial statements or are reasonably likely to affect them in the future, and risks and uncertainties that the issuer believes will materially affect its future performance.

The CSA’s 2016 Staff Notice 11-332 (the “**2016 Staff Notice**”) ⁴⁹, 2017 Staff Notice 33-321 (the “**2017 Staff Notice**”) ⁵⁰ and CSA Multilateral Staff Notice 51-347 (“**MI Staff Notice**”) provide complementary guidance for reporting issuers, registrants, and regulated entities on how to address cyber risk.

In the 2016 Staff Notice, the CSA first provides a summary of its recent initiatives to monitor and address cybersecurity risks in order to improve overall resilience in the public markets and also notes current initiatives on enhancing cross-border information sharing among regulators related to cybersecurity.

The 2016 Staff Notice also provides links and references to a number of particularly helpful cybersecurity resources that have been published by various financial services regulatory authorities and standard-setting bodies in an effort to improve the preparedness of market participants to deal with cyber incidents. Such resources include:

- IIROC Cybersecurity Best Practices Guide^{51 52}
- IIROC Cyber Incident Management Planning Guide⁵³
- Mutual Fund Dealers Association (MFDA) Bulletin #0690-C⁵⁴
- The Office of the Superintendent of Financial Institutions (OSFI) Cybersecurity Self-Assessment Guidance.⁵⁵



The 2017 Staff Notice provides seven distinct areas of guidance based upon a survey of cybersecurity practices that the CSA carried out between October 11, 2016 and November 4, 2016. The survey collected responses from firms registered as investment fund managers, portfolio managers, and exempt market dealers. The purpose of the survey was to gather information about firms' practices in order to permit the CSA to provide effective and useful guidance on how best to guard against cyber risk.

The seven areas of guidance are as follows:

- 1.** Implement policies and procedures that address the 8 following areas and update these policies and procedures frequently, due to ever-changing cyber threats:
 - i.** use of electronic communications;
 - ii.** use of firm-issued electronic devices;
 - iii.** the loss or disposal of an electronic device;
 - iv.** use of public electronic devices or public internet connections to remotely access the firm's network and data;
 - v.** detecting internal or external unauthorized activity on the firm's network or electronic devices;
 - vi.** ensuring software, including anti-virus programs, is updated in a timely manner;
 - vii.** overseeing third-party vendors or service providers with access to the firm's network or data; and
 - viii.** reporting any cybersecurity incidents to the board of directors.
- 2.** Ensure that employees are adequately trained in a firm's cybersecurity practices and schedule cyber training with sufficient frequency to remain current;
- 3.** Carry out a cybersecurity risk assessment at least annually;
- 4.** Develop a written incident response plan to respond to and to escalate a cybersecurity incident;
- 5.** Perform adequate cyber specific due diligence on third-party vendors, consultants and other service providers that have access to a firm's systems and data. Written agreements with such parties should include provisions related to cyber threats;
- 6.** Protect the data. Firms should use encryption for all computers and other electronic devices, and require strong passwords that must be frequently changed to get access to such computers and devices. Data should be backed up regularly and firms should regularly test their back-up process; and
- 7.** Ensure that a firm's insurance policies cover cybersecurity incidents.

The MI Staff Notice, which was adopted by three securities commissions, provides guidance on when to disclose a cybersecurity incident and how to make a determination of materiality that would obligate a reporting issuer to disclose such information in accordance with applicable securities legislation. The MI Staff Notice points issuers to National Policy 51-201, Form 51-102F1, and Form 51-102F2 of National

Instrument 51-102 to assist in making a determination of materiality. It is noted that the materiality will depend on the contextual analysis of the cybersecurity incident and there is no bright-line test or threshold for such incident to reach. In any cyberattack remediation plan, an issuer should include how the materiality of an attack would be assessed.⁵⁶



The SEC has provided similar guidance related to cybersecurity risk disclosure. In February 2018, the SEC released guidance to assist public companies in preparing disclosures about cybersecurity risks and incidents (“**SEC Guidance**”). The SEC Guidance did not propose new rules or rule amendments that would impose new requirements, but rather expressed the SEC’s views within the existing disclosure framework. These views are nevertheless important because SEC staff takes them into consideration when evaluating the adequacy of public company disclosures.⁵⁷

1 Cybersecurity Disclosure Requirements. Given the frequency, magnitude, and cost of cybersecurity incidents, it is critical that public companies take all required actions to inform investors about material cybersecurity risks and incidents in a timely fashion, including those companies that are subject to material cybersecurity risks but may not yet have been the target of a cyberattack. The SEC Guidance provides information for companies on how to address assessments of materiality, a possible duty to correct or update cybersecurity disclosures, and disclosure concerning board oversight of cybersecurity.

2 Materiality. The SEC considers information material if there is a substantial likelihood that a reasonable investor would consider the information important when making an investment decision or disclosure of the information would be viewed by a reasonable investor as having significantly altered the “total mix” of information available. Although the disclosure requirements of Regulation S-K and Regulation S-X do not specifically address cybersecurity risks and incidents, cybersecurity risks or incidents could nevertheless be material depending upon their “nature, extent, and potential magnitude, particularly as they relate to any compromised information or the business and scope of company operations...[and] on the range of harm that such incidents could cause.”

3 Risk Factors. The SEC Guidance flags several cybersecurity risk factors that companies should consider in their form 20-F reporting, including: (i) the probability of the occurrence and potential magnitude of cybersecurity incidents; (ii) the aspects of the company’s business and operations that give rise to material cybersecurity risks and the potential costs and consequences of such risks, including industry-specific risks and third party supplier and service provider risks; and (iii) the potential for reputational harm.

4 Insider Trading & Cybersecurity. The SEC Guidance renews emphasis on the prevention of insider trading in the event of a cybersecurity incident, which could be material non-public information. The SEC suggests that while a company is investigating a cybersecurity incident that has not yet been publicly disclosed, it would be prudent for the company to consider whether to restrict trading by its insiders. This restriction could extend to individuals in IT departments and digital forensics firms who may come across material non-public information in the response to a cybersecurity incident.

The **Office of Compliance Inspections and Examinations (“OCIE”)** has released a report on cybersecurity and resiliency observations. In the report, the OCIE has stated that incident response to cybersecurity incidents includes: (i) timely detection and adequate and appropriate disclosure of material information regarding the incident; and (ii) assessing the appropriate response and corrective action. The OCIE noted that many organizations with an incident response plan include the following elements:



Development of a plan which involves timely notification in the event of an incident, a process to escalate the incident, and communication with key stakeholders;



Addressing applicable reporting requirements including federal and state reporting requirements, such as the filing of a suspicious activity report for financial institutions or disclosure of material risks and incidents for public companies; and



Assigning staff to execute the plan, including specific roles and responsibilities in the event of a cyber incident.⁵⁷

05

Helping You Prepare and Respond

Data incidents at major retailers, government departments, and financial services organizations should serve as a clear warning to all Canadian businesses that handle personal information. Consumers actively expect that these entities should take market-leading steps to protect personal and financial data.

Increasingly, good information management practices go beyond matters of privacy. Malicious hacks (from outside and from within) and ransomware demands have targeted intellectual property, trade secrets, and other critical business information with noticeable impacts on share prices, director and Board longevity, and industry competitiveness. Clients need support from counsel who can marry legislative compliance and the application of industry codes of conduct and privacy policies in various jurisdictions with a practical knowledge of commercial and technology outcomes - all in a manner that will help a client preserve privilege.

Cybersecurity, protection of business information and data, and strategic management of the production and retention of information are all significant aspects of our practice. Our privacy and data management lawyers offer perspective on all aspects of information management, storage, and transfer. Mitigating risk for clients is always our first priority and we have helped clients manage the entire lifecycle of data, including providing guidance to companies looking to prepare for and prevent a critical data incident. When a crisis occurs, we draw from a team of leading class action litigators and subject matter specialists who have responded to some of the highest profile data incidents in North America and are involved in many of the key cybersecurity initiatives (both private and public) in Canada.



Key Contacts



Charles Morgan
Co-Leader, Cyber/Data Group
Partner, Quebec
cmorgan@mccarthy.ca



Dan Glover
Co-Leader, Cyber/Data Group
Partner, Ontario
dglover@mccarthy.ca

Karine Joizil
Preparation & Response | Litigation/
Class Actions | Privacy
Partner, Quebec
kjoizil@mccarthy.ca

Julie-Martine Loranger
Litigation/Class Actions
Partner, Quebec
jmloranger@mccarthy.ca

Emmanuelle Poupart
Litigation/Class Actions | Insurance
Partner, Quebec
epoupart@mccarthy.ca

Isabelle Vendette
Litigation/Class Actions | Privacy |
Preparation & Response
Partner, Quebec
ivendette@mccarthy.ca

Hovsep Afarian
Insurance
Partner, Ontario
hafarian@mccarthy.ca

Heidi Gordon
Preparation & Response |
Corporate Governance &
Public Company Disclosure
Partner, Ontario
hgordon@mccarthy.ca

Nikiforos Iatrou
Competition
Partner, Ontario
niatrou@mccarthy.ca

Christine Ing
Preparation & Response | Privacy
Partner, Ontario
christineing@mccarthy.ca

Gillian Kerr
Litigation/Class Actions
Partner, Ontario
gkerr@mccarthy.ca

Dana Peebles
Preparation & Response |
Litigation/Class Actions
Partner, Ontario
dpeebles@mccarthy.ca

Mike Scherman
Preparation & Response | Privacy
Associate, Ontario
mscherman@mccarthy.ca

Susan Wortzman
E-Discovery | Information Governance
Partner, Ontario
swortzman@mt3.ca

Kara Smyth
Preparation & Response |
Litigation/Class Actions
Partner, Alberta
ksmyth@mccarthy.ca

Shana Wolch
Labour & Employment |
Litigation/Class Actions
Partner, Alberta
swolch@mccarthy.ca

Katherine Booth
Preparation & Response |
Litigation/Class Actions
Associate, British Columbia
kbooth@mccarthy.ca

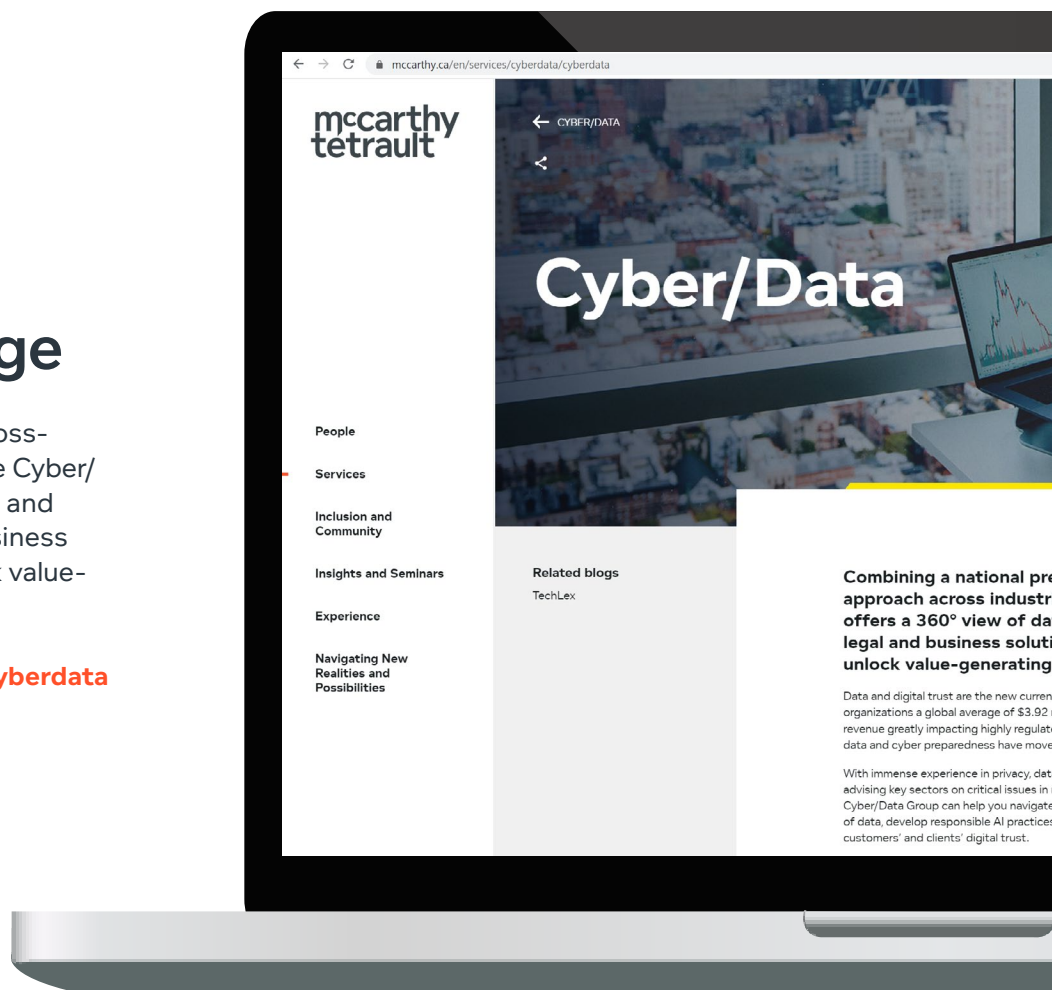
Jade Buchanan
Preparation & Response | Privacy
Associate, British Columbia
jbuchanan@mccarthy.ca

Jill Yates
Litigation/Class Actions
Partner, British Columbia
jyates@mccarthy.ca

Visit Our Webpage

Combining a national presence and cross-practice approach across industries, the Cyber/Data Group offers a 360° view of data and cyber strategy to deliver legal and business solutions that mitigate risks and unlock value-generating potential.

mccarthy.ca/en/services/cyberdata/cyberdata



End Notes

- 1 *Lozanski v The Home Depot, Inc.*, 2016 ONSC 5447 (CanLII), <http://canlii.ca/t/gt65j> at para 70.
- 2 *Personal Information Protection and Electronic Documents Act*, SC 2000, c 5, <http://canlii.ca/t/7vwj>
- 3 “Equifax CEO Richard Smith steps down amid hacking scandal”, *The Washington Post*, September 26, 2017, available at www.washingtonpost.com/news/the-switch/wp/2017/09/26/equifax-ceo-retires-following-massive-data-breach/?noredirect=on&utm_term=.9749ef7df3af.
- 4 “Two Equifax executives resign in wake of massive data breach”, *The Hill*, September 15, 2017, available at <https://thehill.com/policy/cybersecurity/350951-two-equifax-executives-resign-in-wake-of-massive-data-breach>
- 5 Bill 64, *An Act to Modernize Legislative Provisions Respecting the Protection of Personal Information*, which received first reading on June 12, 2020, available at <http://m.assnat.qc.ca/en/travaux-parlementaires/projets-loi/projet-loi-64-42-1.html>.
- 6 PIPEDA, *supra* at section 28.
- 7 See, for example “Privacy Commissioner denounces slow progress on fixing outdated privacy laws”, September 27, 2018, available at https://www.priv.gc.ca/en/opc-news/news-and-announcements/2018/nr-c_180927/ and “Privacy Law Reform - A Pathway to Respecting Rights and Restoring Trust in Government and the Digital Economy”, 019 at https://www.priv.gc.ca/en/opc-actions-and-decisions/ar_index/201819/ar_201819/.
- 8 Cybersecurity Is the Key to Unlocking Demand in the Internet of Things. June 13, 2018. Bain & Company, available at <https://www.bain.com/insights/cybersecurity-is-the-key-to-unlocking-demand-in-the-internet-of-things/>
- 9 From Privacy to Profit: Achieving Positive Returns on Privacy Investments, Cisco Data Privacy Benchmark Study 2020, available at https://www.cisco.com/c/dam/global/en_uk/products/collateral/security/2020-data-privacy-cybersecurity-series-jan-2020.pdf
- 10 For more details, see: Office of the Information and Privacy Commissioner of Alberta, Office of the Privacy Commissioner of Canada and Office of the Information & Privacy Commissioner for British Columbia, “Getting Accountability Right with a Privacy Management Program”, available at: https://www.priv.gc.ca/media/2102/gl_acc_201204_e.pdf
- 11 *Technology and Cyber Security Incident Reporting*. January 2019. Office of the Superintendent of Financial Institutions available at <http://www.osfi-bsif.gc.ca/eng/fi-if/rg-ro/gdn-ort/adv-prv/Pages/TCSIR.aspx>.
- 12 *Ibid.*
- 13 Office of the Superintendent of Financial Institutions Canada, “Memorandum: Cyber Security Self-Assessment Guidance” (October, 2013), available at: <http://www.osfi-bsif.gc.ca/Eng/Docs/cbrsk.pdf>.
- 14 Canadian Securities Administrators, “CSA Staff Notice 33-321: Cyber Security and Social Media” (October, 2017) at 5, available at: https://www.osc.gov.on.ca/documents/en/Securities-Category3/csa_20171019_33-321_cyber-security-and-social-media.pdf
- 15 *Ibid* at 11.
- 16 Drawn from Dennis Palkon et al. v. Stephen P. Holmes et al., No. 2:14-cv-01234 (D.C.N.J., May 2014), the presentation by SEC commissioner Luis A. Aguilar dated June 10, 2014, available at: <http://www.sec.gov/News/Speech/Detail/Speech/1370542057946>, and the National Institute of Standards and Technology’s “Framework for Improving Critical Infrastructure Cybersecurity” (2018), available at <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf>.
- 17 Canadian Cyber Incident Response Centre materials available at <http://www.publicsafety.gc.ca/cnt/ntnl-scrct/cbr-scrct/ccirc-ccric-eng.aspx>.
- 18 “Bank of Canada announces partnership to improve resilience in financial sector”, Bank of Canada, July 2019, available at <http://www.bankofcanada.ca/wp-content/uploads/2014/12/fsr-december14-morrow.pdf>.
- 19 “More Cyber Insurance Buyers as Awareness Grows”, March 2019, Marsh Inc., available at <https://www.marsh.com/us/insights/research/cyber-insurance-trends-report-2018.html>.
- 20 Sasha Romanosky et al, “Content analysis of cyber insurance policies: how do carriers price cyber risk?” (2019) 5:1 J Cybersecurity at 8 to 11, available at: <https://academic.oup.com/cybersecurity/article/5/1/tyz002/5366419>
- 21 Office of the Privacy Commissioner of Canada, available at <https://priv.gc.ca/en>. See, in particular, “What you need to know about mandatory reporting of breaches of security safeguards”, October 2018, available at: https://www.priv.gc.ca/en/privacy-topics/business-privacy/safeguards-and-breaches/privacy-breaches/respond-to-a-privacy-breach-at-your-business/gd_pb_201810/.
- 22 See for example *Ladas v. Apple Inc.*, 2014 BCSC 1821; *Douez v. Facebook, Inc.*, 2014 BCSC 953, which remains in progress (see: 2019 BCSC 715)
- 23 *Li v. Equifax*, 2019 QCCS 4340
- 24 *Ari v. Insurance Corp. of British Columbia*, 2015 BCCA 468.
- 25 *Jones v. Tsige*, 2012 ONCA 32.
- 26 *Agnew-American v. Equifax Canada*, 2018 ONSC 275.
- 27 *Haikola v. The Personal Insurance Company*, 2019 ONSC 5982.
- 28 See, for instance, *Lozanski v The Home Depot, Inc.*, 2016 ONSC 5447 (CanLII), where Perell J. observed that a defendant’s incident response may well be a key factor driving the consideration of the abandonment, discontinuance or settlement of a class action: “The case for Home Depot being culpable was speculative at the outset and ultimately the case was proven to be

- very weak...After the data breach was discovered, there was no cover up, and Home Depot responded as a good corporate citizen to remedy the data breach. There is no reason to think that it needed or was deserving of behaviour modification. Home Depot's voluntarily-offered package of benefits to its customers is superior to the package of benefits achieved in the class actions...By the time the actions against Home Depot came to be settled, there were no demonstrated or demonstrable losses by the Class Members and the Representative Plaintiffs were not even members of the settlement class. Unless one wishes to play pretend, Home Depot was the successful party in resisting a pleaded claim of \$500 million" (at paras 100-101).
- 29 Office of the Privacy Commissioner of Canada. "What you need to know about mandatory reporting of breaches of security safeguards" (October 29, 2018) available at: https://www.priv.gc.ca/en/privacy-topics/privacy-breaches/respond-to-a-privacy-breach-at-your-business/gd_pb_201810/.
- 30 *PIPEDA*, *supra* at section 20(2).
- 31 *Ibid* at section 10.3.
- 32 *Ibid* at section 2(1).
- 33 *Ibid*, at section 10.3(2).
- 34 *Breach of Security Safeguards Regulations*: SOR/2018-64 at section 6.
- 35 Art. 33 GDPR available at: <https://gdpr-info.eu/art-33-gdpr/>.
- 36 Art. 4(21) GDPR defines the "supervisory authority" as an independent public authority which is established by a Member State pursuant to Article 51, online at: <https://gdpr-info.eu/art-4-gdpr/>.
- 37 Art. 4 (7) GDPR for the definition of a "controller" under the GDPR, available at: <https://gdpr-info.eu/art-4-gdpr/>.
- 38 Art. 34 GDPR for more information about the manner of communication to the data subjects and where such communication is not required, available at: <https://gdpr-info.eu/art-34-gdpr/>.
- 39 Art. 83(5) GDPR for more information about administrative fines, available at <https://gdpr-info.eu/art-83-gdpr/>.
- 40 See the following Harvard Business Review article available at: <https://hbr.org/2018/07/what-you-need-to-know-about-californias-new-data-privacy-law>.
- 41 Art. 1798.150 of the California Civil Code, introduced by CCPA.
- 42 *Health Information Act*, RSA 2018 c H-5, Section 42(1).
- 43 See Information and Privacy Commissioner of Ontario, "Report a privacy breach", available at <https://www.ipc.on.ca/health-organizations/report-a-privacy-breach/>.
- 44 PCI Security Standards, May 2018 available at: https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2-1.pdf?agreement=true&time=1594333796156.
- 45 *Ibid*.
- 46 PCI Security Standards Council, PCI Forensic Investigators, available at: https://www.pcisecuritystandards.org/as-sessors_and_solutions/pci_forensic_investigators.
- 47 "SEC Investigative Report: Public Companies Should Consider Cyber Threats When Implementing Internal Accounting Controls", United States' Securities and Exchange Commission (16 October 2018), available at: <https://www.sec.gov/news/press-release/2018-236>.
- 48 SEC, Commission Statement and Guidance on Public Company Cybersecurity Disclosures, February 2018, available at: <https://www.sec.gov/rules/interp/2018/33-10459.pdf>.
- 49 CSA Staff Notice 11-332: Cyber Security (27 September 2016), available at: https://www.osc.gov.on.ca/documents/en/Securities-Category1/sn_20160927_11-332-cyber-security.pdf
- 50 CSA Staff Notice 33-321: Cyber Security and Social Media (19 October 2017), available at: https://www.osc.gov.on.ca/documents/en/Securities-Category3/csa_20171019_33-321_cyber-security-and-social-media.pdf.
- 51 Available at http://www.iiroc.ca/industry/Documents/CybersecurityBestPracticesGuide_en.pdf.
- 52 On November 14, 2019, the Investment Industry Regulatory Organization of Canada ("IIROC") issued an amendment which came into effect immediately, that required all investment dealers regulated by IIROC to report all cybersecurity incidents, available at: https://www.iiroc.ca/documents/2019/d73ffdfa-819e-4560-992b-162d1e2a9c0f_en.pdf.
- 53 Available at http://www.iiroc.ca/industry/Documents/CyberIncidentManagementPlanningGuide_en.pdf.
- 54 Available at <http://mfda.ca/bulletin/Bulletin0690-C/>.
- 55 Available at <http://www.osfi-bsif.gc.ca/eng/fi-if/in-ai/pages/cbrsk.aspx>.
- 56 CSA Multilateral Staff Notice 51-347: Disclosure of cyber security risks and incidents (19 January 2017), available at: https://www.osc.gov.on.ca/documents/en/Securities-Category5/20170119_51-347_disclosure-cyber-security.pdf.
- 57 SEC, Commission Statement and Guidance on Public Company Cybersecurity Disclosures, February 2018, available at: <https://www.sec.gov/rules/interp/2018/33-10459.pdf>.
- 58 SEC, Cybersecurity and Resiliency Observations: Office of Compliance Inspections and Examinations (2019), available at: <https://www.sec.gov/files/OCIE%20Cybersecurity%20and%20Resiliency%20Observations.pdf>.

VANCOUVER

Suite 2400, 745 Thurlow Street
Vancouver BC V6E 0C5

CALGARY

Suite 4000, 421 7th Avenue SW
Calgary AB T2P 4K9

TORONTO

Suite 5300, TD Bank Tower
Box 48, 66 Wellington Street West
Toronto ON M5K 1E6

MONTREAL

Suite 2500
1000 De La Gauchetière Street West
Montréal QC H3B 0A2

QUÉBEC CITY

500, Grande Allée Est, 9e étage
Québec QC G1R 2J7

NEW YORK

55 West 46th Street, Suite 2804
New York, New York 10036
United States

LONDON

1 Angel Court, 18th Floor
London EC2R 7HJ
United Kingdom