About Blakes Cybersecurity Practice

Blakes has one of the largest and most active cybersecurity practices in Canada. Our national and bilingual team assists clients with developing and implementing risk-mitigation strategies, acts as breach counsel in the event of a cybersecurity incident and represents clients of all sizes in the event of regulatory investigations or litigation.

Our team has advised on some of the most complex cybersecurity incidents in Canada and has successfully represented clients in class-action litigation. Our practice and members of our team have been consistently recognized as leading experts in this area by Chambers Global: The World’s Leading Lawyers for Business and The Best Lawyers in Canada.

For further information about our Cybersecurity practice, visit www.blakes.com/cybersecurity
Introduction ........................................................... 2
Methodology ........................................................... 2
Cyber Snapshot .......................................................3

Part 1: Cybersecurity Incidents ......................... 4
1. Of the cybersecurity incidents reported, what is the breakdown by industry? ................. 4
2. What were the leading types of cyber threats encountered in 2019? .......................... 4
3. Where did the cybersecurity incident occur? ...... 5
4. When dealing with a cybersecurity incident, which vendors did you call upon? .............. 5
5. In the event of ransomware attacks, what percentage of organizations paid the ransom? .... 6
6. Where a ransom payment was made, what was the average payment amount? ............... 6
7. What was the primary impact of the cybersecurity incident on your organization? ........ 6
8. What is the average time for a business to recover from a cybersecurity incident? .......... 7
9. What type of data did hackers have access to? ... 7
10. Was the cybersecurity incident reported to law enforcement? .................................... 8
11. Did the organization have standalone cyber insurance in place? ..................................... 8
12. Did the organization have a Cybersecurity Incident Response Plan (CIRP) in place that it followed when dealing with the cybersecurity incident? .............................................. 8

Part 2: Privacy Breaches ................................. 9
Data Breaches Reported Under Privacy Legislation 9
Breach Reporting Trends Under PIPEDA and Privacy Act ................................................. 10
Breach Reporting Under Provincial Laws (Private Sector) ................................................. 10

Part 3: Public Company Disclosure Trends ......... 11
Overview .............................................................. 11
1. Lack of Internal Cybersecurity Policies .......... 12
2. Insufficient Employee Training and Awareness .... 12
3. Low Take-Up of Cyber Insurance .................... 12
4. Low Executive Oversight ................................. 12
5. Few Designated Chief Cybersecurity Officers in Place .............................................. 12
6. Few Organizations Are Following National Best Practice Guidelines ....................... 12
7. Inadequate Data Encryption Measures ............ 12
8. Gas, Oil and Consumable Fuels Industries Are Further Advanced .......................... 12

Part 4: Cybersecurity Litigation Trends ............ 13

Contact Us............................................................ 14
Introduction

In recent years, the number of cybersecurity incidents reported in Canada and across the globe has continued to grow at an alarming pace. The potential effects to businesses resulting from a major cybersecurity incident can include financial loss, operational disruption and reputational harm, not to mention lengthy regulatory investigations and litigation. Familiarizing oneself with the types of cyber threats that an organization faces is a key factor in being prepared for a cyber security incident.

Unfortunately, there is a paucity of current and reliable Canada-specific data when it comes to the types of cyber threats that organizations face, their frequency, impact and other indicators that assist organizations in preparing for a potential cybersecurity incident.

This first edition of our annual Blakes Canadian Cybersecurity Trends Study focuses on providing readers with an overview of the key trends we are observing in Canada. The study covers three broad categories of trends: (1) cybersecurity incidents, (2) privacy breaches, and (3) cybersecurity-related disclosures by public companies. We invite you to review the results of the study that we hope will provide valuable insights to help you develop or update your cybersecurity preparedness strategy.

Methodology

Part 1 of the study is based on a survey of cybersecurity forensic firms that responded to more than 250 cybersecurity incidents across Canada. The data obtained covered the period from January 1, 2019, to October 15, 2019, roughly 10 months.

Part 2 of the study is based on a review of publicly released data by the federal, Alberta and British Columbia privacy commissioners’ offices. This included reviewing historical data and is current up to November 1, 2019. Information for Quebec was unavailable.

Part 3 of the study is based on a review of various public-disclosure documents (e.g., annual report, annual information form, management discussion and analysis, management information circular and final long-form prospectus) of the 790 corporate issuers listed on the Toronto Stock Exchange (TSX) for cybersecurity-related disclosure statements. The information is taken from 2018/2019 SEDAR filings for these companies.
Cyber Snapshot

Financial, health and professional services are more likely to be targeted by hackers given the quantity of sensitive information they hold (including personal information of employees and customers).

Ransomware (35%) and Business Email Compromise (24%) attacks were the top two cyber threats in 2019.

More than half (53%) of organizations that were victim of a ransomware attack opted to pay a ransom.

The top three impacts of a major cybersecurity incident were operational disruption (33%), financial loss (25%) and negative impact on relationships with business partners (21%).

Since November 1, 2018, when the federal mandatory breach notification came into force, there has been a six-fold increase in privacy breaches reported to the Office of the Privacy Commissioner of Canada.

Only 29% of organizations had an effective Cybersecurity Incident Response Plan (CIRP) that they used to respond to the cybersecurity incident.

Less than a third (31%) of organizations reported a cybersecurity incident to law enforcement.

A little over 10% of publicly listed companies have indicated that they have standalone cyber insurance in place.

Only 41% of publicly listed companies indicated they had some sort of internal cybersecurity policy in place.

About a third (31%) of publicly listed companies indicated they have a committee in place responsible for actively overseeing the organization’s cybersecurity management.
Part 1: Cybersecurity Incidents

1) Of the cybersecurity incidents reported, what is the breakdown by industry?

Hackers continue to target industries that have access to large amounts of personal or sensitive data (finance, health, and professional services). These industries are highly regulated, and a major cybersecurity incident can trigger significant reporting obligations to affected individuals and regulatory bodies, not to mention class action proceedings.

Ransomware continues to be a leading threat to organizations, especially since it often relies on human error. We have observed that more sophisticated ransomware variants are emerging at an accelerated rate.

Interestingly, “business email compromise” (also known as “BEC” incidents) has also emerged as a major threat to organizations. We have noted a significant increase in the number of BEC incidents in the second half of 2019.

2) What were the leading types of cyber threats encountered in 2019?
3) Where did the cybersecurity incident occur?

On a relative basis, hackers do not appear to be targeting a particular region of Canada. Hacker campaigns against a particular industry remain a rare occurrence. There have been, however, some notable exceptions over the past year, namely campaigns targeting municipalities and health care service providers in Canada.

* Western Canada includes Alberta, Manitoba and Saskatchewan
** Atlantic Canada includes New Brunswick, Newfoundland & Labrador, Nova Scotia and Prince Edward Island

4) When dealing with a cybersecurity incident, which vendors did you call upon?

In most instances, organizations reached out to specialized cybersecurity firms to assist them in containing the incident, remediating and conducting a forensic investigation. Also, more than half of the organizations called upon external legal counsel to assist them with their cyber response.
5) In the event of ransomware attacks, what percentage of organizations paid the ransom?

Approximately half of organizations opted to pay a ransom demanded by hackers. It is noteworthy that the decision to pay was often related to the type of ransomware. For example, ransomware attacks involving sophisticated variants such as Ryuk and Bitpaymer often resulted in organizations opting to make a ransom payment.

6) Where a ransom payment was made, what was the average payment amount?

Approximately 70% of ransoms paid were less than C$100,000. These payments are often made via bitcoin payment, a digital crypto currency that allows the hackers to remain anonymous. It is noteworthy that in many instances, following “negotiations” with the hacker, the ransom amount paid is often lower than what the hackers had initially demanded. However, as 2019 progressed we saw an increase in the quantum of the ransom amounts being demanded and paid.

7) What was the primary impact of the cybersecurity incident on your organization?

The leading impact on organizations is operational disruption, meaning that the organization cannot carry out its day-to-day operations. This is closely linked to financial loss. Given the interconnectivity of businesses and the rise of “just in time” supply models, a significant operational disruption will also impact B2B relationships where the victim organization will often need to disclose the nature and scope of the cybersecurity incident to a business partner.
8) What is the average time for a business to recover from a cybersecurity incident?

<table>
<thead>
<tr>
<th>Recovery Time</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt; 1 week</td>
<td>15%</td>
</tr>
<tr>
<td>1-2 weeks</td>
<td>28%</td>
</tr>
<tr>
<td>2-4 weeks</td>
<td>24%</td>
</tr>
<tr>
<td>&gt; 4 weeks</td>
<td>23%</td>
</tr>
</tbody>
</table>

Approximately half of organizations that suffered a cybersecurity incident took over two weeks to recover. Almost a quarter needed more than a month. While the recovery time varied based on the type of cybersecurity incident and the complexity of the organization's IT environment, key factors that impacted recovery time included the need to conduct a forensic investigation, secure all affected systems and bring systems back online in a manner that ensured network stability.

9) What type of data did hackers have access to?

- Personal Information (Customer): 15%
- Personal Information (Employee): 16%
- Corporate Data (Sensitive): 28%
- Corporate Data (Non-Sensitive): 12%
- Other: 10%
- No Data Affected: 19%

Forensic investigations often revealed that hackers had access to different categories of data but that they were primarily interested in accessing personal information as well as sensitive corporate data. The latter category was of interest to hackers so they could commit financial fraud.

*Occurs where an internal or external malicious actor steals personal information that was in the possession of an organization*
10) Was the cybersecurity incident reported to law enforcement?

- Yes: 31%
- No: 69%

Over two-thirds of cybersecurity incidents were not reported to law enforcement.

11) Did the organization have standalone cyber insurance in place?

- Yes: 14%
- No: 86%

While cyber insurance is viewed as a component of a company’s cyber-risk mitigation strategy, the actual number of companies that had this type of coverage in place prior to the cybersecurity incident was quite low. This type of insurance has been steadily growing in Canada and typically covers the costs of legal, forensics, crisis communications and cyber extortion.

12) Did the organization have a Cybersecurity Incident Response Plan (CIRP) in place that it followed when dealing with the cybersecurity incident?

- Yes: 29%
- No: 71%

A large majority of organizations either did not have or did not rely on their CIRP to respond to the cybersecurity incident. The absence of an effective and practical CIRP when dealing with a cybersecurity incident can result in undue delays, confusion and an overall ineffective response to the incident.
Part 2: Privacy Breaches

Data Breaches Reported Under Privacy Legislation


As of November 1, 2018, organizations that are subject to the federal Personal Information Protection and Electronic Documents Act (PIPEDA) are required to notify the Office of the Privacy Commissioner (OPC) and affected individuals of a “breach of security safeguards” involving personal information that poses a real risk of significant harm to an individual.

Approximately 680 reports were filed with the OPC. Based on these reports, at least 28 million Canadians were potentially affected by a privacy breach. A breakdown of the 680 reports filed is provided below:

<table>
<thead>
<tr>
<th>Type of Incident</th>
<th>Number of Reports</th>
<th>Percentage (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unauthorized Access</td>
<td>394</td>
<td>58</td>
</tr>
<tr>
<td>Theft*</td>
<td>54</td>
<td>8</td>
</tr>
<tr>
<td>Loss**</td>
<td>82</td>
<td>12</td>
</tr>
<tr>
<td>Accidental Disclosure***</td>
<td>150</td>
<td>22</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td>680</td>
<td>100</td>
</tr>
</tbody>
</table>

Since November 1, 2018, there has been a six-fold increase in the number of breach reports filed with the OPC as compared with the immediately prior year.

* Occurs where an internal or external malicious actor steals personal information that was in the possession of an organization

** Occurs where an organization accidentally or inadvertently loses personal information in its possession

*** Occurs where an organization accidentally discloses personal information to an unauthorized third-party
PART 2: PRIVACY BREACHES

Breach Reporting Trends Under PIPEDA and Canada’s Federal Privacy Act*

In the 2017-2018 fiscal year, 116 breaches under PIPEDA and 286 breaches under the Privacy Act were reported to the OPC.

Breach Reporting Under Provincial Laws (Private Sector)

British Columbia, Alberta and Quebec have each enacted privacy laws substantially similar to PIPEDA which apply to private sector organizations.

The British Columbia Personal Information Protection Act, the Alberta Freedom of Information and Protection of Privacy Act and the British Columbia Freedom of Information and Protection of Privacy Act provide for voluntary breach reporting.

The Alberta Personal Information Protection Act was the first private-sector general applicable privacy law to introduce mandatory breach notification by the private sector. This requirement was introduced in 2010.

In Quebec, the Act Respecting the Protection of Personal Information in the Private Sector provides for voluntary breach notification. However, the Quebec provincial government has announced that it will be introducing a new privacy law that will impose mandatory breach notification.

Between 2012 to 2018, British Columbia and Alberta have essentially seen a consistent year-over-year increase (with the exception of 2013-2014 in Alberta) in the number of breaches reported to the provincial privacy commissioners’ offices.

Data regarding the number for the breaches reported to Quebec’s Commission d’accès à l’information du Québec was not available.

2020 BLAKES CANADIAN CYBERSECURITY TRENDS STUDY
### Part 3: Public Company Disclosure Trends

#### Overview

Blakes reviewed the disclosure documents of the 790 corporate issuers listed on the TSX for cybersecurity-related disclosure statements. We have identified 137 companies that have issued some type of cybersecurity-related statement. This represents less than 20% of all TSX corporate issuers. However, 92 companies (out of the 137) are S&P/TSX Composite Index members that have a total market capitalization of $1.7 trillion (or 60% of the total market capitalization on the TSX) which highlights the importance of cybersecurity for Canada’s largest issuers.

The breakdown below relates to the 137 companies that disclosed cyber risk:

<table>
<thead>
<tr>
<th>Industry</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Energy</td>
<td>29</td>
</tr>
<tr>
<td>Materials</td>
<td>13</td>
</tr>
<tr>
<td>Banks</td>
<td>10</td>
</tr>
<tr>
<td>Diversified Financials</td>
<td>8</td>
</tr>
<tr>
<td>Real Estate</td>
<td>7</td>
</tr>
<tr>
<td>Software and Services</td>
<td>7</td>
</tr>
<tr>
<td>Capital Goods</td>
<td>7</td>
</tr>
<tr>
<td>Insurance</td>
<td>7</td>
</tr>
<tr>
<td>Utilities</td>
<td>7</td>
</tr>
<tr>
<td>Transportation</td>
<td>6</td>
</tr>
<tr>
<td>Food, Beverage and Tobacco</td>
<td>4</td>
</tr>
<tr>
<td>Commercial and Professional Services</td>
<td>4</td>
</tr>
<tr>
<td>Media and Entertainment</td>
<td>4</td>
</tr>
<tr>
<td>Telecommunication Services</td>
<td>4</td>
</tr>
<tr>
<td>Pharmaceuticals, Biotechnology &amp; Life Sciences</td>
<td>4</td>
</tr>
<tr>
<td>Retailing</td>
<td>3</td>
</tr>
<tr>
<td>Automobiles and Components</td>
<td>2</td>
</tr>
<tr>
<td>Technology Hardware and Equipment</td>
<td>2</td>
</tr>
<tr>
<td>Consumer Services</td>
<td>2</td>
</tr>
<tr>
<td>Multi-Utilities</td>
<td>2</td>
</tr>
<tr>
<td>Real Estate</td>
<td>2</td>
</tr>
<tr>
<td>Consumer Durables and Apparel</td>
<td>1</td>
</tr>
<tr>
<td>Food and Staples Retailing</td>
<td>1</td>
</tr>
<tr>
<td>Health Care Equipment and Services</td>
<td>1</td>
</tr>
</tbody>
</table>
Our review highlighted the following trends for public companies that have issued some type of cybersecurity-related statement.

1. **Lack of Internal Cybersecurity Policies**
   Only 41% of companies indicated they had some sort of internal cybersecurity policy in place.

2. **Insufficient Employee Training and Awareness**
   Only a third of companies indicated that their employees participate in cybersecurity training and awareness programs.

3. **Low Take-Up of Cyber Insurance**
   Only 12% of companies indicated that they have some form of cyber insurance leaving them exposed to potentially significant costs upon the occurrence of an attack. This is consistent with our observations in Part 1.

4. **Low Executive Oversight**
   Roughly a third (31%) of companies indicated they have a committee in place responsible for actively overseeing the organization's cybersecurity management.

5. **Few Designated Chief Cybersecurity Officers in Place**
   Only 5% of companies indicated they have a chief security officer (or similar position) who is appointed with the specific role of overseeing the organization's cybersecurity management. We expect this number to grow in the coming years.

6. **Few Organizations Are Following National Best Practice Guidelines**
   Only 6% of companies reported that they follow the National Institute of Standards and Technology (NIST) cybersecurity guidelines. The NIST standards are viewed as being “minimal” standards that organizations should have in place.

7. **Inadequate Data Encryption Measures**
   A mere 11% of companies indicated they have encryption measures in place to protect confidential information.

8. **Gas, Oil and Consumable Fuels Industries Are Further Advanced**
   These critical infrastructure organizations tend to be better prepared than companies in other industries, although a lot of work remains to be done. A good 52% of these companies indicated the following:
   - They maintain policies and procedures to address and implement employee protocols with respect to electronic communications and electronic devices and conduct annual cybersecurity risk assessments.
   - They employ encryption to protect confidential information, all computers and other electronic devices.
   - Despite their efforts to mitigate cyber-phishing attacks through education and training, cyber-phishing activities remain a serious problem that may damage their information technology infrastructure.
   - They apply technical and process controls in line with industry-accepted standards to protect their information, assets and systems, including a written incident-response plan for responding to a cybersecurity incident.
In 2018 and 2019, we observed the following trends in cybersecurity-related litigation matters:

1. **Increase in privacy class actions in Canada**
   
   There has been an increasing number of privacy class actions in Canada since 2012, when the Ontario Court of Appeal first recognized the new privacy tort of intrusion upon seclusion. Privacy class actions have been certified in most provinces, particularly Ontario, British Columbia and Quebec.

   In 2018 and 2019, at least three class proceedings arising out of cybersecurity incidents were certified (not including cases certified for the purposes of settlement). Other privacy class actions involving theft or unauthorized use of data by employees were certified as well.

   In that same period, courts refused to certify three proposed class actions arising out of cybersecurity incidents. These denials of certification suggest that courts are increasingly willing to scrutinize plaintiffs’ claims to assess whether they are viable.

2. **Privacy commissioner investigations.**
   
   The federal and provincial privacy commissioners are taking an increasingly active role in investigating cybersecurity incidents. We expect this trend to continue under the mandatory notification regime (see page 9).

   In 2019, the Office of the Privacy Commissioner of Canada (OPC) released three investigation reports relating to specific cyber-attacks, one of which was a joint investigation with a provincial privacy commissioner. By comparison, no such reports were released in 2018 or 2017. The OPC conducted many other investigations in this period that have not yet resulted in a published report.

3. **Continued uncertainty about liability for cyber-attacks by third parties.**
   
   To date, no privacy class action in Canada has proceeded to a determination on the merits. It remains to be seen whether plaintiffs will ultimately be able to recover damages, particularly in cases where the defendant has been the victim of a cyber-attack perpetrated by a third party.

4. **Settlement values in privacy class actions.**
   
   There have been a handful of settlements of privacy class actions. Most settlements in cases involving large-scale criminal cyber-attacks have represented low values per claimant (in the range of C$15 to C$100 per person allegedly affected).

   However, 2018 and 2019 saw some higher-value settlements approved in cases involving deliberate breaches of highly sensitive personal information, with payments to class members of up to C$2,750 in one case involving a deliberate intrusion on sensitive medical records by a rogue employee.

5. **Effective breach responses may mitigate risk.**
   
   A prompt and effective response to a cybersecurity incident can preserve reputation and goodwill. It may also mitigate litigation risk, including by preventing losses to affected individuals. Judges have commented favourably on the quality of the defendant’s response to cybersecurity incidents in decisions not to certify a proposed class proceeding and approving early settlements.
This Study is intended for informational purposes only and does not constitute legal advice or an opinion on any issue.

We would be pleased to provide additional details or advice about specific situations if desired.

For permission to reprint, please contact the Blakes Client Relations & Marketing department at communications@blakes.com.