Blakes

Canadian Cybersecurity Trends Study

2021

About Blakes Cybersecurity Practice

The Blakes Cybersecurity group is one of Canada's largest cybersecurity legal teams with operations in each of Blakes Canadian offices. Using innovative and cutting-edge tools, our experienced team advises clients at all points along the cyber-risk spectrum: from risk mitigation training and incident response to regulatory investigations, board preparedness and litigation. Our Cybersecurity team has extensive experience in crisis management when clients fall victim to data and security breach incidents.

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*, *The Best Lawyers in Canada* and a host of other recognized legal ranking organizations in Canada and globally.

For further information about our Cybersecurity practice, visit **www.blakes.com/cybersecurity**

Blakes | Blakes Means Business

Contents

CANADIAN CYBERSECURITY TRENDS STUDY 2021

Introduction

Were it not for the COVID-19 pandemic, cybersecurity would have ranked at the top of key governance issues faced by organizations in 2020.

While the number of cybersecurity incidents reported in Canada had been growing at an alarming pace in previous years, Canada experienced exponential growth in cyber-attacks on organizations, government and individuals. The first quarter of 2021 was no different, with the trend continuing at the same exponential and alarming pace.

Introduction

The increased sophistication of attacks, coupled with more individuals working remotely due to the pandemic, seems to have created the perfect storm for general counsel, chief privacy officers, chief information security officers and others responsible for preventing and responding to cyber-attacks and other data-related incidents. The pandemic accelerated the digitization of almost every aspect of our lives, requiring the rapid introduction of new technologies into both our work and personal lives. We are now experiencing the associated cybersecurity fallout of a rapidly organized digitized world. Accordingly, the need for better cyber preparedness and vigilance across all industries and organizations has become an imperative.

Without appropriate cybersecurity protocols, organizations cannot adequately prepare for cyber-attacks and, if exposed, may face significant financial loss, reputational harm, operational disruption and potential lengthy regulatory investigations and litigation.

Appropriate cybersecurity protocols can be informed by trends in the cybersecurity landscape, yet there is a lack of current and reliable Canada-specific data. To address the current paucity in national private-sector data, we present our second annual *Canadian Cybersecurity Trends Study*.

As with our inaugural edition, our goal is to provide readers with an overview of the key trends we are observing in Canada. Our study covers four broad categories of trends: (1) cybersecurity incidents, (2) privacy breaches reported to federal and provincial commissioners, (3) cybersecurity-related disclosures by Canadian public companies, and (4) cybersecurity litigation trends. A glossary of cybersecurity terms is included at the end of the report.

We invite you to review the results of the study for valuable insights to help you develop or update your cybersecurity-preparedness strategy.

We remind our readers that one of the most important things an organization can do to properly secure itself against cyber threats is to maintain vigilance. This means continually refreshing policies, being mindful about the introduction of new systems and processes within the organization and ongoing training. The only way to ensure cybersecurity is with sufficient measures, continuous attention and the right resources.

Methodology

As with our inaugural study, we have separated this year's edition into discrete parts and rely on pictograms and charts to ensure that the data is easily digestible.

Part 1 is based on an aggregation of data from forensic firms that responded to cybersecurity incidents across Canada, combined with aggregated observations from the large number of breaches that were handled by the Blakes Cybersecurity team. The data analyzed in the study covers the period from September 1, 2019, to December 31, 2020.

Part 2 is based on a review of publicly released data by the federal, Alberta and British Columbia privacy commissioners' offices, including historical data. It is current up to November 1, 2020. Information for Quebec was unavailable.

Part 3 is based on a review of various public-disclosure documents of the 763 corporate issuers listed on the Toronto Stock Exchange (TSX) for cybersecurity-related disclosure statements. The documents include annual report, annual information form, management discussion and analysis, management information circular and final long-form prospectus. The information is taken from 2020 SEDAR filings for these companies.

Part 4 is based on trends observed by the Blakes Cybersecurity group. Litigation related to cyber and data breaches is becoming more prevalent. While these are still early days, one can already see the early development of trends in the approaches taken by litigants and the courts.

We received a great deal of positive feedback following the inaugural release of our study in 2020, with clients noting their appreciation for the study and how it filled an important niche in the Canadian marketplace. Acknowledging this, our Cybersecurity team worked even harder on this year's report, which we proudly share with you. We trust you will find the study useful in helping you consider your organization's approach to cybersecurity.

Cyber Snapshot

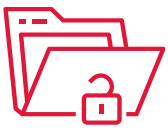
Key findings from this year's analysis.

Ransomware (67%) and business email compromise (18%) attacks ranked as the top two most common cyber incidents in 2020.

In 52% of cyber incidents, the threat actor obtained unauthorized access to data as opposed to merely encrypting the data for a simple ransomware attack.

In over half of ransomware attacks (54%), the victim opted to pay the ransom.

Approximately 60% of the ransom payments that were made were greater than US$100,000. In some cases, ransoms in the millions of dollars are now being paid. This presents a notable increase in the quantum being demanded by threat actors. The dramatic increase in ransom costs also had some expected follow-on effects in the insurance industry — cyber insurance, an important aspect of many organization's cyber strategy, is becoming both more sophisticated and expensive.



With respect to cybersecurity policies, 40% of publicly listed companies report not having one.

Only 17% of publicly listed companies indicated that they have some form of cyber insurance, leaving them exposed to potentially significant costs upon the occurrence of an attack.

01

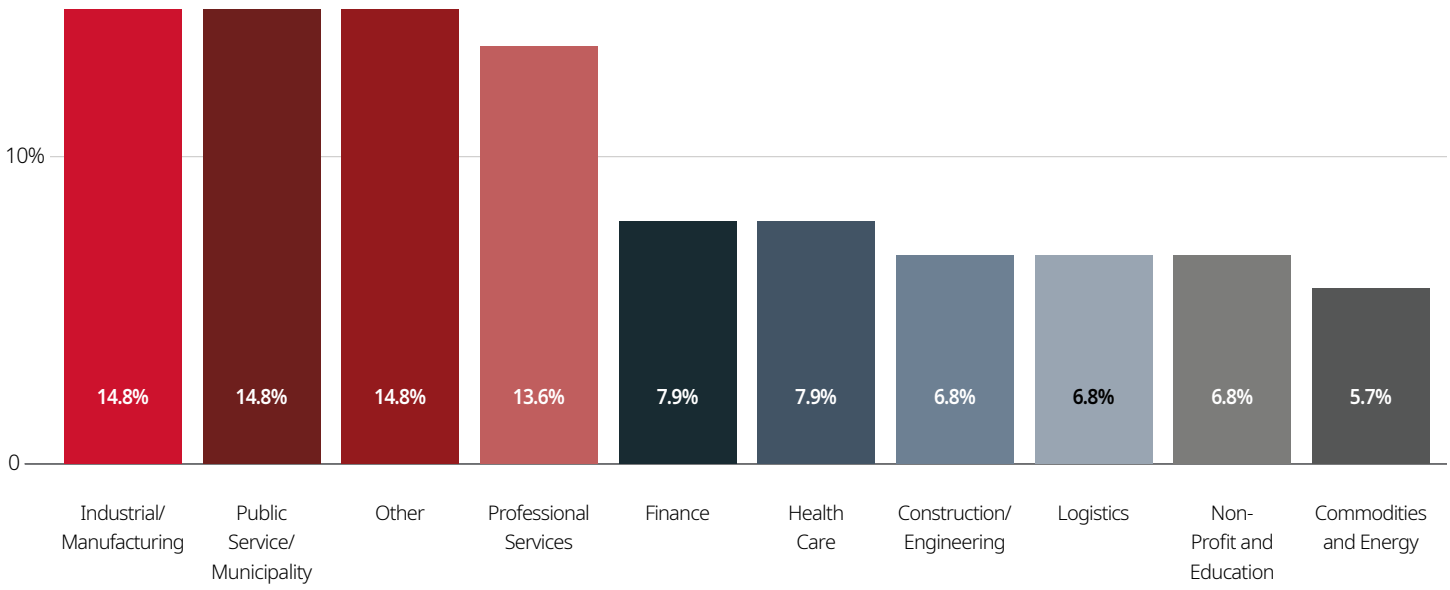
CANADIAN CYBERSECURITY TRENDS STUDY 2021

Cybersecurity Incidents

In this section, we have reviewed data collected from forensic firms dealing with cybersecurity incidents across Canada, combined with aggregated observations from a large number of breaches handled by the Blakes Cybersecurity team. The data analyzed covers the period from September 1, 2019 to December, 31 2020.

Cybersecurity Incidents

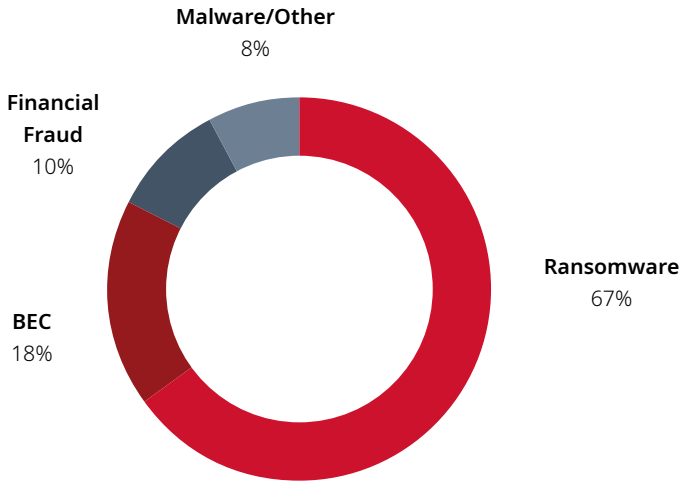
1) Of the cybersecurity incidents reported, what is the breakdown by industry?



While cyber-attacks are industry agnostic, certain industries like manufacturing, public services and professional services appear to have been targeted to a greater degree by threat actors than other industries.

While all industries are vulnerable to a cyber-attack, the impact felt by organizations following such incidents is not uniform. Industries in which the collection and storage of personally identifiable information is common, such as health, finance and professional services, are increasingly facing complicated and burdensome regulatory notification requirements in the event of a loss of control of their data.

2) What was the nature of the incident?

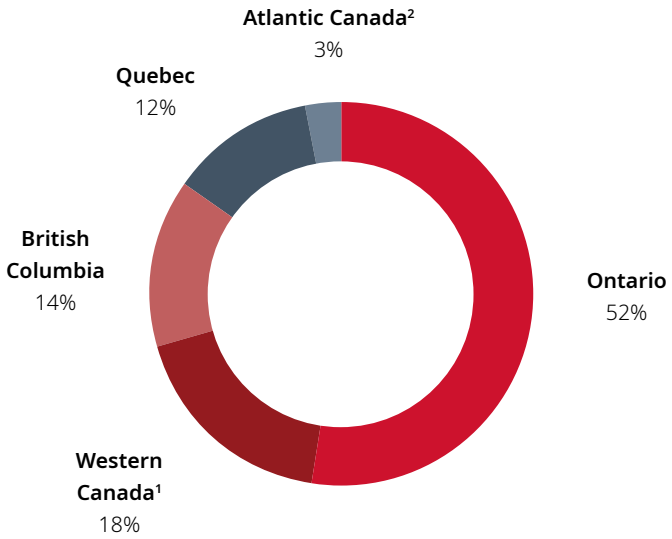


Ransomware attacks continue to be the leading type of cybersecurity incident. In fact, the proportion of ransomware incidents has increased. In 2019, ransomware attacks represented 35% of cybersecurity incidents, and in 2020, they represent 67% of cybersecurity incidents. This is not surprising given that ransomware attacks are generally the easiest for threat actors to carry out. A ransomware attack can easily shut down an entire organization.

While business email compromises (BECs) represent a smaller proportion of incidents (decreasing from 24% in 2019 to 18% in 2020), they are often more complicated and expensive to deal with. We expect that a significant number of such attacks will continue to plague Canadian organizations in the coming years. As with ransomware attacks, BECs do not require overly sophisticated tactics and can wreak havoc in an organization.

Finally, and while still a smaller percentage of attacks, following the well-publicized Solar Winds incident, certain hacking groups are carrying out extremely sophisticated attacks on network and other forms of infrastructure. These groups typically distinguish themselves from the typical ransomware or BEC threat actors by the sophistication of their techniques, their patience in conducting the attack over long periods of time and the goal of the attack, which may not be financial but rather related to espionage or bringing down infrastructure.

3) Where did the cybersecurity incident occur?

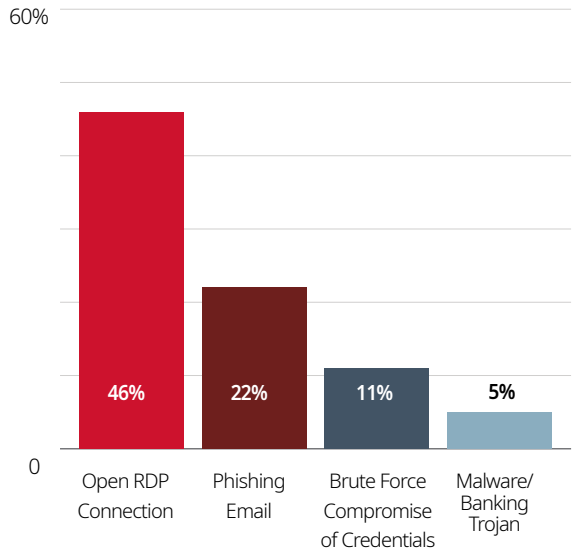


Our data indicated a higher number of attacks in Ontario relative to its population size particularly when compared to Quebec. However, the data was not as skewed when Ontario was compared to the rest of the country. We believe this to be the result of incomplete data with respect to Quebec-based attacks and not due to a targeting of a particular region of Canada. It is our opinion that threat actors do not seem to be discriminating by region.

[1] Western Canada includes Alberta, Manitoba and Saskatchewan

[2] Atlantic Canada includes New Brunswick, Newfoundland & Labrador, Nova Scotia and Prince Edward Island

4) How was the threat actor able to compromise the environment?



Almost half of all attacks were a result of an open remote desktop protocol (RDP) connection. RDP is a key component of enabling remote work, allowing employees to connect to their organization while outside the four walls of their office and continue their jobs as normally as possible. This finding is notable as it confirms that threat actors have been able to successfully exploit the rise in employees working remotely as a result of the COVID-19 pandemic and social-distancing measures.

5) Was the threat actor able to access any data during the attack?

48% No

52% Yes

In a little more than half of the cybersecurity incidents we reviewed, the threat actor successfully accessed data. Organizations should be aware that, in most circumstances, unauthorized access to personal information entails reporting to one or more Canadian privacy commissioners and other regulators. It also involves sending notification requirements to affected individuals if there is a real risk of significant harm.

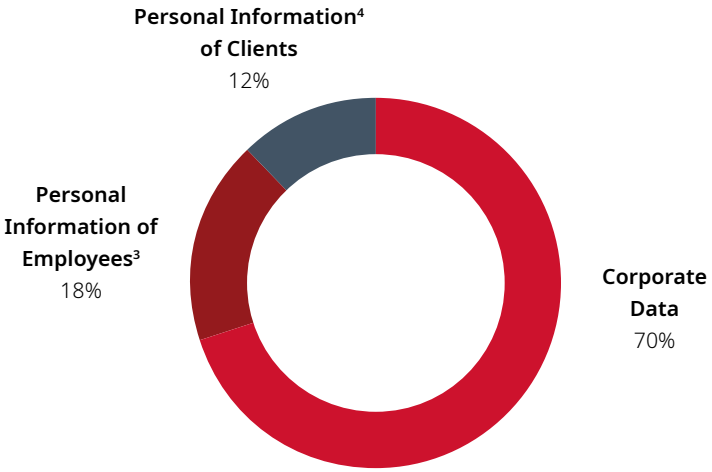
6) Was the threat actor able to exfiltrate (i.e. remove) any data during the attack?

While many attacks result in the threat actor accessing data during an attack, exfiltration occurs less often. Still, we found that exfiltration occurred in about a third of the attacks.

72% No

28% Yes

7) If data was accessed or exfiltrated, what was the nature of that data?



Approximately 70% of unauthorized access and exfiltration involves corporate data. While a data breach solely involving corporate data does not trigger notification and reporting obligations under Canadian privacy law, the loss of control of this information can nevertheless be financially devastating to an organization.

[3] Whether or not corporate data was also affected

[4] Whether or not corporate data and/or personal information of employees was also affected

8) In the event of a ransomware attack, what percentage of organizations paid the ransom?

46% No

54% Yes

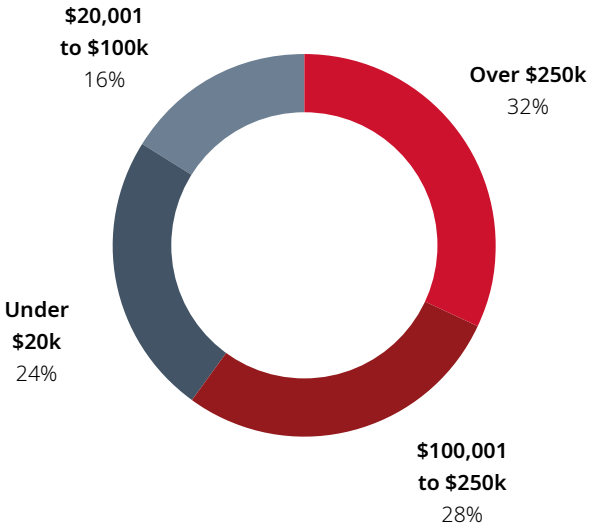
Approximately half of organizations opted to pay a ransom that was demanded by the threat actor. This is consistent with what we observed in 2019. It is noteworthy that there is no clear correlation between the ransomware variant (i.e., malware type) and the decision to pay. That is, ransomware incidents where the threat actor demanded a relatively low payment do not more frequently result in organizations opting to pay. Increasingly, threat actors are exfiltrating data prior to encrypting an organization's systems to enhance their chances of being paid the ransom. The tactic from the threat actor's perspective is that even though an organization might be able to restore their backups, thus obviating the need for a decryption key, they may nonetheless pay the ransom so that the data that was exfiltrated is not released.

9) Where a ransom payment was made, what was the payment amount (USD)?

60% of the ransom payments that were made were greater than US$100,000. We note that there have been significant increases in the price of ransom demands in 2020 as compared to 2019.

It is often possible to negotiate ransom amounts with the threat actors to lower the final amount that is transferred. Both the initial amounts demanded and the actual amounts paid to threat actors have increased over the past year.

Threat actors typically demand that these payments be made using a cryptocurrency such as Bitcoin or Monero, allowing the threat actors to remain anonymous.



10) If a ransom was paid, did the threat actor provide functional decryption keys and/or evidence of data deletion?

9% No

91% Yes

In most cases when a ransom was paid, the threat actor "held up their end of the bargain." That is, when a payment was made in exchange for functional decryption keys or deletion of all exfiltrated data, the threat actor provided the keys or evidence that the exfiltrated data was deleted. Although it may seem surprising, hacking groups have reputations to maintain. A hacking group that cannot be trusted to fulfil its end of the bargain once a ransom is paid may find it difficult to have future ransoms paid as the cybersecurity community is small and word gets out quickly. Generally speaking, the well-known hacking groups that have some longevity hold up their end of the bargain.

11) What ransomware variant was responsible for the attack?

The number of ransomware variants observed is growing year over year. Here are some of the variants that were active during the period we studied:

Bitpaymer	Egregor	Maze	Pysa
Buran	Lazange	Medusa	Ragnar
Conti	LockBit	NetWalker	Ryuk
Cuba	Mamba	Ourobouros	Snatch
Dharma	Matrix	Phobos	Sodinokibi
DopplePaymer			

12) Was the incident reported to law enforcement?

89% No

11% Yes

Nearly 90% of cybersecurity incidents were not reported to law enforcement.

13) Was the incident reported to a Canadian (federal or provincial) Privacy Commissioner?

90% No

10% Yes

The majority (90%) of cybersecurity incidents were not reported to the Office of the Privacy Commissioner of Canada or one of its provincial counterparts. While cybersecurity incidents are required to be reported to a privacy commissioner by law only under certain conditions, organizations may choose to voluntarily report incidents.

14) Were any individuals notified of the incident?

Organizations will only be legally required to notify affected individuals of a cybersecurity event under certain conditions. In some cases, organizations voluntarily choose to notify all or some of the affected individuals even if they are not legally required to (often with an offer to pay for credit monitoring if identification or financial data was accessed).

82% No

18% Yes

15) Did the organization have and follow a cyber incident response plan (CIRP)?

96% No

4% Yes

The majority of organizations did not either have or rely on a CIRP to respond to the cybersecurity incident.

Preparing to respond to a cybersecurity incident can help identify weaknesses in an organization's security systems, allowing the organization to make adjustments to reduce the likelihood of one happening. As mentioned at the outset of this study, preparation requires resources in terms of time, personnel and money, and should not be taken lightly.

02

CANADIAN CYBERSECURITY TRENDS STUDY 2021

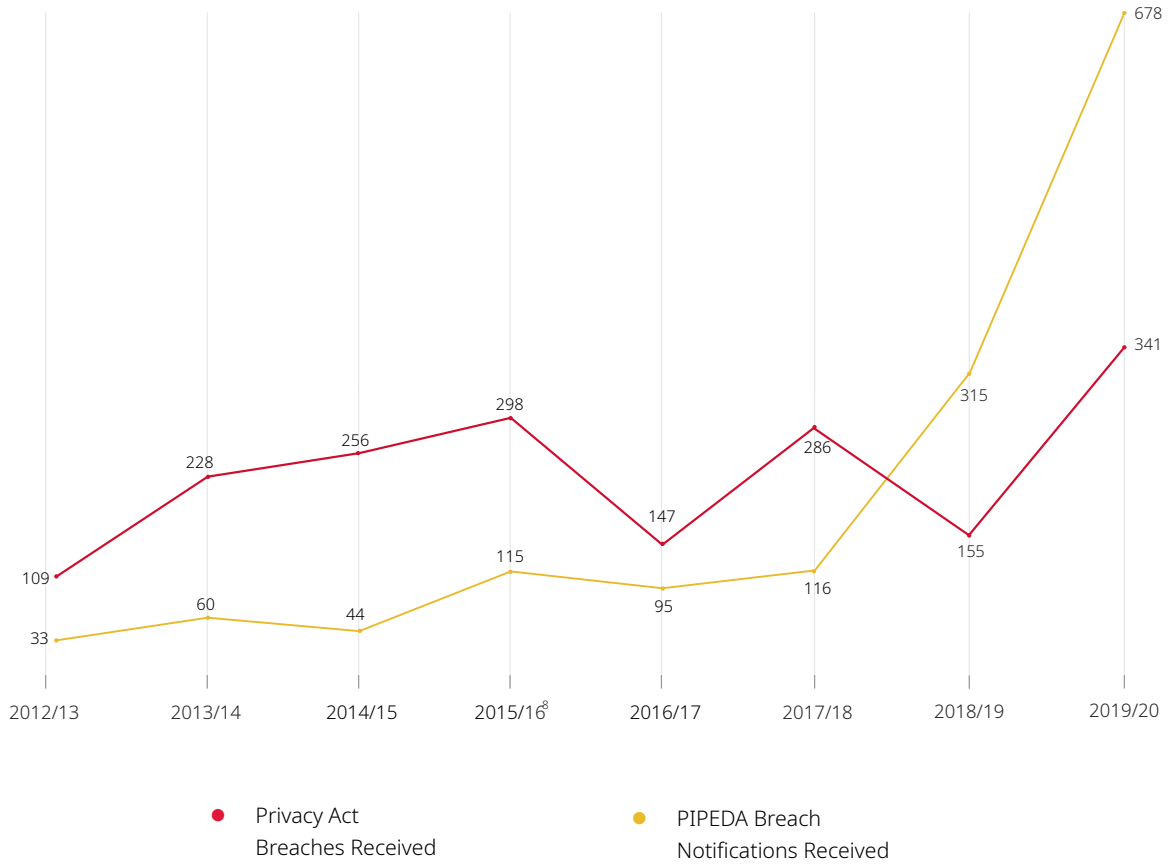
Privacy Breaches

In this section, we have analyzed publicly released data from the federal, Alberta and British Columbia privacy commissioners' offices, including historical data. It is current up to November 1, 2020. Information for Quebec was unavailable.

Privacy Breaches

Breach Reporting Trends Under PIPEDA and Canada's Federal Privacy Act

In the 2019-2020 fiscal year, **678 breaches** governed by the private-sector *Personal Information Protection and Electronic Documents Act* (PIPEDA)[5,6] and **341 breaches** governed by the federal public-sector *Privacy Act*[7] were reported to the Office of the Privacy Commissioner of Canada (OPC).



5 *Personal Information Protection and Electronic Documents Act*, SC 2000, c 5.

6 On November 17, 2020, Bill C-11, the *Digital Charter Implementation Act, 2020* was introduced in the House of Commons. If passed, this highly anticipated bill would overhaul the federal government's approach to regulating privacy in the private sector. This would include introducing new administrative monetary penalties of up to the greater of C$10-million or 3% of the organization's total global revenues for the prior financial year for contravention of certain provisions of the new statute, including failure to protect personal information through physical, organizational and technological security safeguards and failure to notify the Commissioner and affected individuals of a breach if there is a real risk of significant harm. The potential fines for offences contrary to the new law also increase from the C$100,000 potential fine under PIPEDA to the higher of C$25-million or 5% of gross global revenues. The offences subject to such fines include failure to report or keep records of a data breach; *Blakes Bulletin: New Federal Bill Set to Reform Canada's Private-Sector Privacy Laws*.

7 *Privacy Act*, RSC 1985, c P-21.

8 The 2015-2016 PIPEDA statistics were for a 15-month period.

Highlights: Privacy-Sector Breach Reporting

While every year the number and magnitude of data breaches grows, November 1, 2018, marked the beginning of mandatory breach reporting under PIPEDA. Since then, the OPC has seen significant increases in the number of breach reports they receive.

In 2019-2020, the OPC received 678 breach reports affecting 30 million Canadians' accounts, which is more than double the number of reports received during the previous year and six times the amount the OPC received the year before breach reporting became mandatory.[9]

In 2019-2020, the majority of breach-incident reporting involved unauthorized access. A breakdown of the 678 reports filed is provided below:

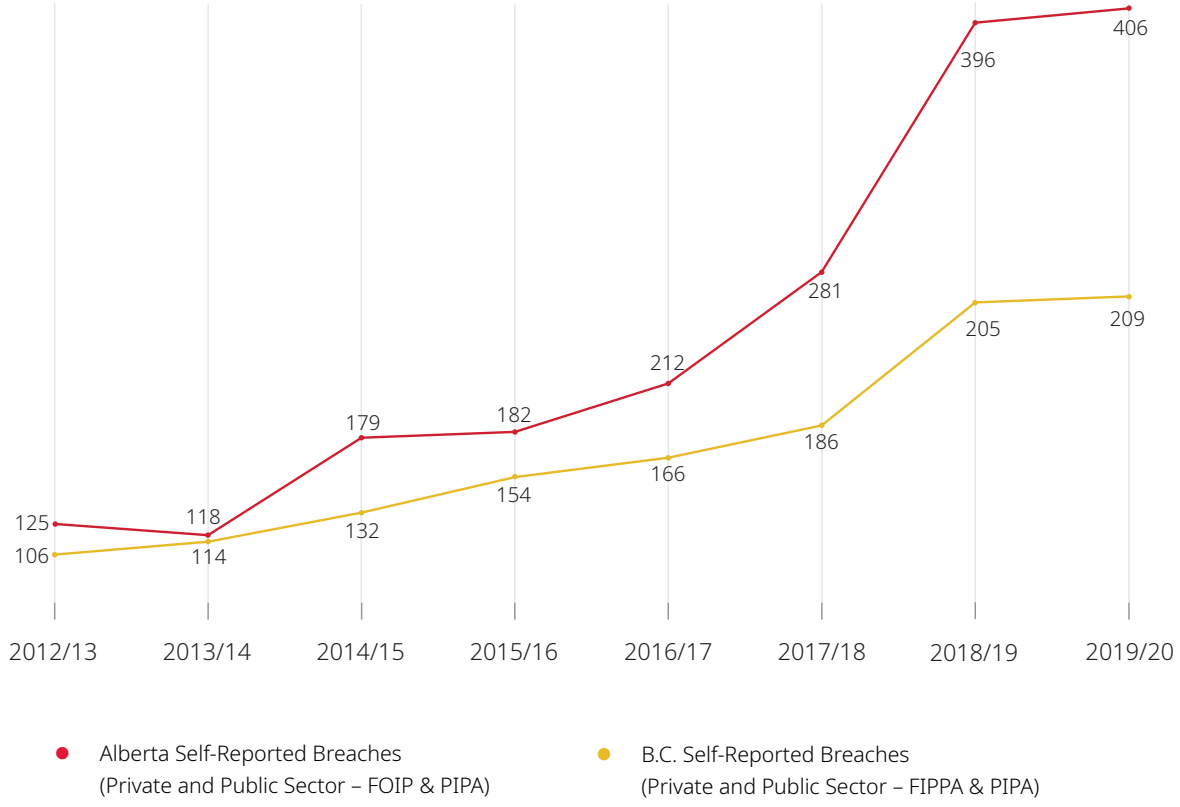
Type of Incident	Number of Incidents	Percentage of Incidents
Unauthorized Access (including malware, ransomware, password attacks, etc.)	402	59.3%
Accidental disclosure	144	21.2%
Loss	72	10.6%
Theft	60	8.8%
Total	**678**	**100%**

While the 2019-2020 period witnessed an increased number of breach reports from the public sector, the OPC continues to be concerned about systemic underreporting in the public sector.[10] The OPC has noted that several large institutions, including the Canada Border Services Agency, Department of National Defence, Global Affairs Canada and Veterans Canada have been conspicuously absent from the breach reports the OPC receives.

[9] Privacy in a pandemic - Office of the Privacy Commissioner of Canada
[10] Privacy in a pandemic - Office of the Privacy Commissioner of Canada

Breach Reporting Under Provincial Laws (Private Sector)

British Columbia, Alberta and Quebec have each enacted privacy laws substantially similar to PIPEDA that apply to private-sector organizations.[11] Every province also has public-sector privacy legislation.



Alberta's private-sector *Personal Information Protection Act*[12] was the first generally applicable privacy law to introduce mandatory breach notification. This requirement was introduced in 2010.

The British Columbia private-sector *Personal Information Protection Act*,[13, 14] the Alberta public-sector *Freedom of Information and Protection of Privacy Act* [15] and the British Columbia public-sector *Freedom of Information and Protection of Privacy Act*[16] provide for *voluntary* breach reporting.

Between 2012 and 2020, British Columbia and Alberta have essentially seen a consistent year-over-year increase (with the exception of 2013 to 2014 in Alberta) in the number of breaches reported to the provincial privacy commissioners' offices.

In Quebec, the *Act Respecting the Protection of Personal Information in the Private Sector*[17] provides for voluntary breach notification. However, the Quebec provincial government has announced that it will be introducing new privacy legislation that will impose mandatory breach notification.

11 We have not included statistics relating to the personal health information legislation that many provinces have also enacted.

12 *Personal Information Protection Act*, SA 2003, c P-6.5.

13 *Personal Information Protection Act*, SBC 2003, c 63.

14 In February, the Legislative Assembly of British Columbia appointed a special committee to review the *Personal Information Protection Act*; Blakes Bulletin: Canadian Privacy Law 2020 Year in Review

15 *Freedom of Information and Protection of Privacy Act*, RSO 1990, c F.31.

16 *Freedom of Information and Protection of Privacy Act*, RSBC 1996, c 165.

17 *Act Respecting the Protection of Personal Information in the Private Sector*, CQLR c P-39.1.

03

CANADIAN CYBERSECURITY TRENDS STUDY 2021

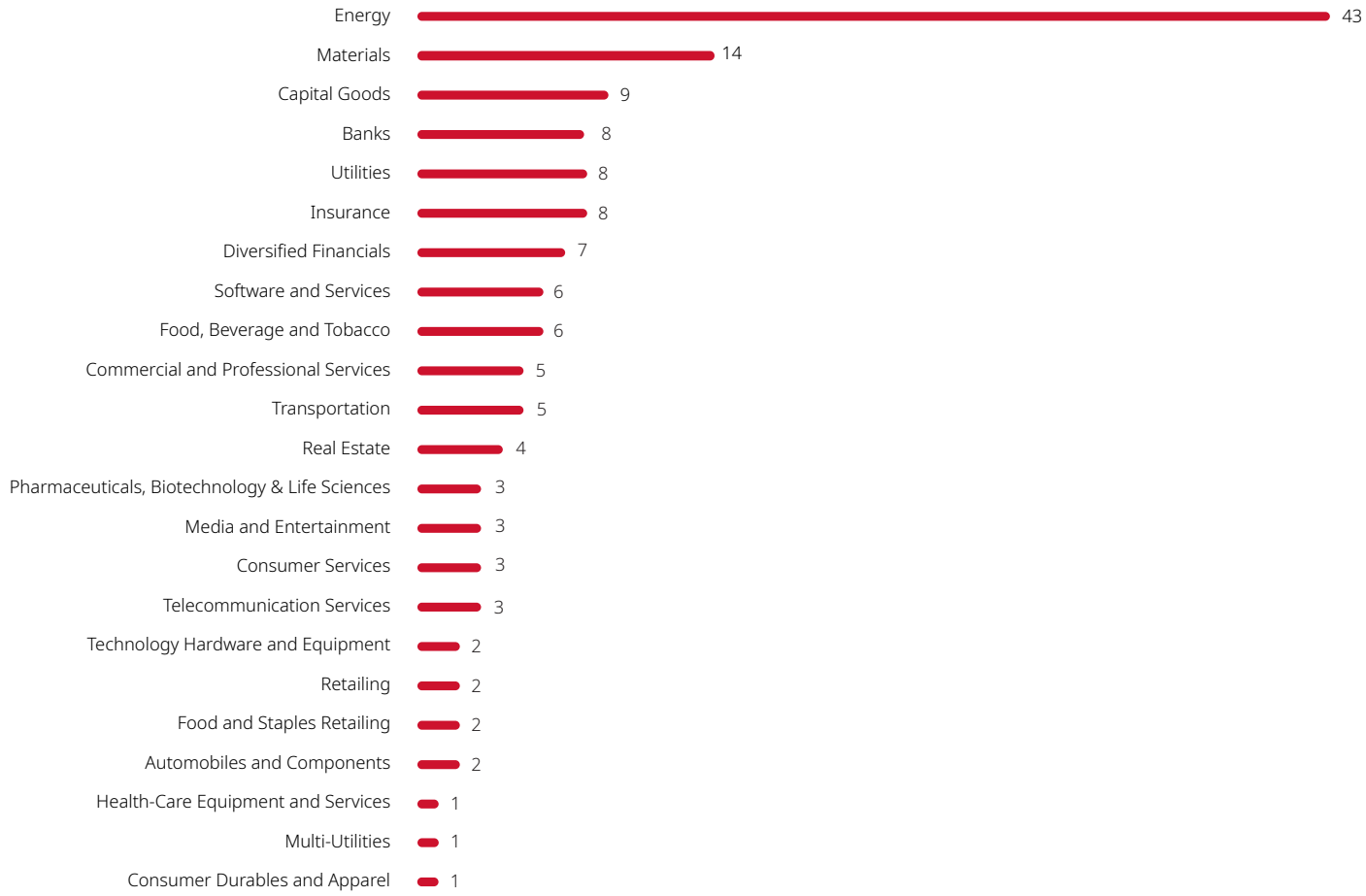
Public Company Disclosure Trends

In this section, we have reviewed various public disclosure documents of the 763 corporate issuers listed on the Toronto Stock Exchange (TSX) for cybersecurity-related disclosure statements. The information is taken from 2020 SEDAR filings for these companies.

Public Company Disclosure Trends

Blakes reviewed the disclosure documents of the 763 corporate issuers listed on the TSX for cybersecurity-related disclosure statements. We have identified 146 companies that have issued some type of cybersecurity-related statement. This represents nearly 20% of all TSX corporate issuers. However, 80 companies (out of the 146) are S&P/TSX Composite Index members that have a total market capitalization of C$1.7-trillion (or 50% of the total market capitalization on the TSX), which highlights the importance of cybersecurity for Canada's largest issuers.

The industry breakdown below represents the 146 companies that disclosed cyber risk:



Our review highlighted the following trends for public companies that have issued some type of cybersecurity-related statement.

1. Increasing Recognition of Benefit of Internal Cybersecurity Policies

60% of companies indicated they had some sort of internal cybersecurity policy in place. This is a significant increase compared to 41% in 2019.

Implementation of a cyber policy meaningfully assists organizations in effectively managing their cyber risk. A comprehensive cyber policy will outline:

- Technology and information assets that you need to protect
- Threats to those assets
- Rules and controls for protecting the assets and your business

2. Lack of Board Cybersecurity-Risk Oversight

Only 26% of companies indicated that they have a chief security officer or a designated committee of directors to manage cybersecurity risk.

Boards can play a key role in setting the tone that cybersecurity is a critical business issue. They can also be instrumental in helping management create a cybersecurity framework with the appropriate risk appetite.

3. Low Take-Up of Cyber Insurance

Only 17% of companies indicated that they have some form of cyber insurance leaving them exposed to potentially significant costs upon the occurrence of an attack. The financial and industrial sectors have the most issuers (seven and six, respectively) maintaining standalone cyber-insurance policies.

Cyber insurance can cover regulatory and civil litigation defence expenses, civil damages, crisis management expenses, forensic investigation expenses, security-breach remediation and notification expenses, ransom payments, business interruptions, and crisis management expenses.

4. Reported Cyber Incidents

Only four companies reported having experienced a cyber incident in their 2020 filing. Three of these incidents were ransomware attacks that resulted in electronic data encryption. Note that attacks that were not considered by a publicly listed company to be material may not have been reported.

5. Cyber Incident Response Plan/Disaster Recovery Plan

Approximately 23% of companies indicated that they have some form of written cyber incident response plan (CIRP) or disaster recovery plan.

A CIRP should be documented to provide a well-defined, flexible and organized approach for handling any potential threats to computers, networks and data, as well as taking appropriate action if the source of an intrusion or incident at a third party is traced back to the organization. A CIRP should include steps to identify, contain, eradicate, communicate and recover from cyber incidents.

7. Inadequate Data Encryption Measures

A mere 17% of companies indicated that they maintain encryption protection measures for confidential and sensitive information.

Encryption is one of the many ways to protect data. It can also be secured through a variety of other measures, including multi-factor authentication, strong firewalls, antivirus protection, regular back-ups, etc. Organizations should consider the sensitivity of the data they store and ensure appropriate security measures.

6. Employee Training

One third of companies indicated that their employees have participated in cybersecurity training and awareness programs.

Regular employee training should be widely adopted as it is integral to building a culture of security in modern, digitally dependent organizations.

8. Gas, Oil and Consumable Fuel Industries Are Further Advanced

These critical infrastructure organizations tend to be better prepared than companies in other industries. However, **only a third** of these companies indicated all four of the following (with 68% indicating that they complied with the first two bullet points below).

- 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 on 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.

04

CANADIAN CYBERSECURITY TRENDS STUDY 2021

Cybersecurity Litigation Trends

In this section, we discuss trends observed by the Blakes Cybersecurity and Data Breach Response & Litigation team.

Cybersecurity Litigation Trends

01 Privacy Class Actions in Canada

The proliferation of privacy class actions continues across Canada. In 2020, at least one privacy class action was certified following a contested hearing. A handful of certification motions in cases arising out of cybersecurity incidents are set to be heard in 2021. Certification has already been refused in two cases, one in Alberta because the plaintiff could not prove harm, and one in Ontario because the plaintiff had no evidence that data had been shared.

In one significant appellate decision in 2020, the British Columbia Court of Appeal upheld certification of a data breach class action and suggested that intrusion upon seclusion may become a viable cause of action in that province. Appeals are pending in several privacy class-action cases in other provinces. These may give appellate courts opportunities to restate or clarify the legal principles that apply in privacy cases, particularly regarding the scope of the tort of intrusion upon seclusion, which was only introduced into the Ontario common law in 2012.

In spring 2021, a privacy class action in Quebec was dismissed on its merits at a rare common issues trial because the plaintiff did not prove that any of the affected data was used unlawfully. To date, no privacy class action in any of the common law provinces has been determined on the merits. It remains to be seen whether plaintiffs will be able to recover damages, particularly when the defendant is a victim of a third-party cyber-attack.

02 Privacy Commissioner Investigations

The federal and provincial privacy commissioners have taken an active role in the investigation of cybersecurity incidents in 2020. The Office of the Privacy Commissioner of Canada (OPC) released three investigation reports relating to cyber-attacks in 2020, all of which were conducted jointly with one or more other provincial privacy commissioners. In 2020, the OPC also released, jointly with two provincial commissioners, an investigation report relating to the unauthorized mass collection of digital personal information. The OPC conducted many other investigations in 2020, some of which have not yet resulted in published reports.

With the proposed changes to privacy legislation federally and in some provinces, we expect the OPC and other provincial privacy commissioners to be even more active in enforcement.

03 Settlement Values in Privacy Class Actions

Settlements in cases involving large-scale criminal cyber-attacks continue to return fairly low values per claimant (in the range of C$15 to C$100 per person allegedly affected). However, there have been some higher-value settlements approved in cases involving deliberate breaches of highly sensitive personal information. In 2020, there was an increased use of cy-près distributions of settlement funds (i.e., to non-profit organizations rather than the affected individuals) where damage to claimants was minimal or non-existent. We expect this trend to continue.

04 Director and Officer Liability

As of 2020, individual directors and officers have begun to be named as defendants in Canadian privacy class actions. Claims against individual directors and officers of a company have become increasingly common in data breach litigation in the United States. While these claims have sometimes been struck out at an early stage, some U.S. courts have more recently permitted director and officer liability claims to proceed to determination on their merits. No Canadian case has yet decided whether directors or officers can be liable for data breaches or cyber-attacks on a corporation, or in what circumstances.

05 Expert Reports and Privilege

No Canadian court has made a definitive ruling on whether expert reports prepared following a data breach are protected by privilege. However, in 2020, American courts ordered production of forensic reports in a handful of cases, as did one provincial privacy commissioner. This underscores the importance of using best practices to protect privilege in breach investigations.

CANADIAN CYBERSECURITY TRENDS STUDY 2021

Glossary

A summary of common cybersecurity-related terms and definitions

Glossary

Term	Definitition
Business email compromise (BEC)	A cybersecurity incident whereby an organization's email is used to carry out the attack. This includes sending phishing emails and financial fraud attempts.
Cyber incident response plan (CIRP)	A plan that helps an organization prepare for and respond to cybersecurity incidents.
Data access	Occurs where a threat actor can view, copy or manipulate data stored on an organization's systems.
Data exfiltration	Occurs where a threat actor can make a copy of an organization's data on their own systems. The data leaves the organization's systems and is reproduced on a storage system controlled by the threat actor.
Decryption key	A tool that may be provided by a threat actor upon payment that allows the affected organization to decrypt the affected files and systems, thereby making them accessible to the organization.
Phishing email	An email that is designed to obtain sensitive information, such as passwords or financial information, by giving the appearance of being from a trusted sender.
Ransomware	A type of malware that renders an organization's systems or files inaccessible, often by encrypting them, until a ransom is paid. In some cases, ransomware may also have other effects, including exfiltrating data from the affected systems.
Ransomware variant	A type of ransomware. Variants are characterized by the software that is used in the attack as well as the group that executes it.
Threat actor	The individual or group that is responsible for a cybersecurity incident.

Key Contacts

If you have any questions, please get in touch with any of our key contacts on the following page.

Key Contacts

Vancouver

Alexandra Luchenko
604-631-4166
alexandra.luchenko@blakes.com

Montréal

Sunny Handa
514-982-4008
sunny.handa@blakes.com

Marie-Hélène Constantin
514-982-4031
mariehelene.constantin@blakes.com

Calgary

Alyssa Duke
403-260-9748
alyssa.duke@blakes.com

Birch Miller
403-260-9613
birch.miller@blakes.com

Renee Reichelt
403-260-9698
renee.reichelt@blakes.com

Toronto

Catherine Beagan Flood
416-863-2269
cbe@blakes.com

David Feldman
416-863-4021
david.feldman@blakes.com

Iris Fischer
416-863-2408
iris.fischer@blakes.com

Nicole Henderson
416-863-2399
nicole.henderson@blakes.com

Wendy Mee
416-863-3161
wendy.mee@blakes.com

Robert Percival
416-863-5297
robert.percival@blakes.com