Catalogue no. 85-002-X
ISSN 1209-6393

Juristat

Cyber security and cybercrime challenges of Canadian businesses, 2017

by Howard Bilodeau, Mohammad Lari and Mark Uhrbach
The Canadian Centre for Justice Statistics

Release date: March 28, 2019

Statistics Canada Statistique Canada

Canada

How to obtain more information

For information about this product or the wide range of services and data available from Statistics Canada, visit our website, www.statcan.gc.ca.

You can also contact us by

email at STATCAN.infostats-infostats.STATCAN@canada.ca

telephone, from Monday to Friday, 8:30 a.m. to 4:30 p.m., at the following numbers:

• Statistical Information Service	1-800-263-1136
• National telecommunications device for the hearing impaired	1-800-363-7629
• Fax line	1-514-283-9350

Depository Services Program

• Inquiries line	1-800-635-7943
• Fax line	1-800-565-7757

Standards of service to the public

Statistics Canada is committed to serving its clients in a prompt, reliable and courteous manner. To this end, Statistics Canada has developed standards of service that its employees observe. To obtain a copy of these service standards, please contact Statistics Canada toll-free at 1-800-263-1136. The service standards are also published on www.statcan.gc.ca under "Contact us" > "Standards of service to the public."

Note of appreciation

Canada owes the success of its statistical system to a long-standing partnership between Statistics Canada, the citizens of Canada, its businesses, governments and other institutions. Accurate and timely statistical information could not be produced without their continued co-operation and goodwill.

Published by authority of the Minister responsible for Statistics Canada

An HTML version is also available.

Cette publication est aussi disponible en français.

Cyber security and cybercrime challenges of Canadian businesses, 2017: Highlights

- Just over one-fifth (21%) of Canadian businesses reported that they were impacted by cyber security incidents which affected their operations in 2017 compared with 23% of businesses in the United Kingdom.
- More than half (54%) of impacted businesses in Canada reported that cyber security incidents prevented employees from carrying out day-to-day work, while close to one-third (30%) experienced additional repair or recovery costs.
- About 10% of businesses in Canada reported that they lost revenue as a result of cyber security incidents and fewer (6%) businesses reported that the incidents damaged the reputation of their business.
- Sectors in Canada which reported the highest level of incidents included banking institutions (excluding investment banking) (47%), universities (46%) and pipeline transportation (45%). Businesses in these sectors were mostly impacted by incidents to steal money or demand ransom payments in 2017.
- For all types of incidents, 65% of Canadian businesses reported that they believed an external party was responsible for the cyber security incidents.
- About 10% of Canadian businesses impacted by a cyber security incident reported the incident to a police service in 2017.
- The vast majority (94%) of businesses in Canada had some level of expenditure to prevent or detect cyber security incidents in 2017. On average, Canadian businesses spent $78,000 on implementing such measures. This was mainly driven by the average expenditure of large businesses ($922,000) and medium-sized businesses ($108,000). Small businesses reported spending an average of $44,000.
- The majority of large (91%), medium-sized (83%) and small (72%) businesses in Canada reported having employees primarily responsible for the overall cyber security of their business in 2017. Additionally, the use of consultants or contractors to manage cyber security risks and threats was also prevalent. About 45% of medium-sized businesses used the services of consultants and contractors in comparison to 38% of large businesses and 33% of small businesses.
- Very few (5%) Canadian businesses reported not having any cyber security measures to protect themselves, their customers and their partners. In addition to the cyber security measures in place, over half (58%) of the businesses undertook activities to identify cyber security risks.

Cyber security and cybercrime challenges of Canadian businesses, 2017

by Howard Bilodeau, Mohammad Lari and Mark Uhrbach

Canadian businesses continue to rapidly embrace the Internet and digital technologies, which has the potential to expose them to greater cyber security risks and threats. However, the impact of these risks and threats on the investment and day-to-day decisions of businesses are not easily understood as cyber security incidents often go unreported (van der Meer 2015).

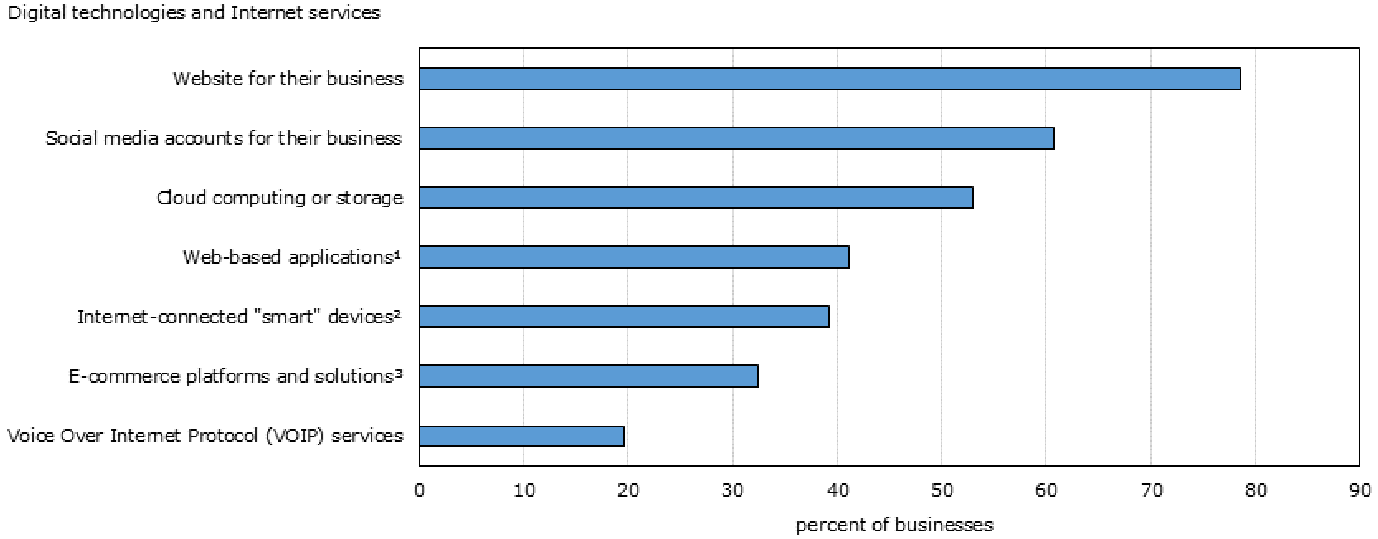
This *Juristat* article uses information collected through the Canadian Survey of Cyber Security and Cybercrime (CSoCC), the first official statistical release of its kind in Canada, to examine some of these data gaps and provide new and current insights into the behaviour of Canadian businesses as they meet the cyber security challenges of a changing world.[1]

The paper begins by looking at how businesses are exposed to cyber security risks and threats through their use of digital technologies and services that are connected to the Internet. It further explores the impact cybercrime had on business operations in 2017 and the reporting practices of businesses after the incident. Finally, the article examines the types of investments businesses had made to manage these risks and threats through the types of cyber security measures they employed.

Vast majority of businesses rely on digital technologies and services

The growing reliance of businesses on digital technologies and services that are connected to the Internet exposes them to greater cyber security risks. About 92% of Canadian businesses reported using one or more digital technologies or services in 2017.[2] Close to 80% of businesses had a website in 2017, and 61% of businesses had a social media account. The use of such technologies appears to have risen greatly since 2013 when 46% of businesses reported having a website and about 38% of such businesses integrated it with their social media accounts (Statistics Canada 2013a; Statistics Canada 2013b).[3] A large proportion of businesses now also use other technologies such as cloud computing or storage services (53%) and Internet-connected 'smart' devices (39%) (Chart 1).

Chart 1
Types of digital technologies and Internet services used, Canada, 2017



1. For example, payroll processing, electronic signature, order and delivery service applications.
2. For example, smart televisions, Wi-Fi enabled security cameras.
3. For example, online payment and ordering.
Source: Statistics Canada, Canadian Survey of Cyber Security and Cybercrime.

As the dependencies on digital technologies and services connected to the Internet and to each other continues to grow, the risk of such technologies and services being manipulated by unauthorized parties increases correspondingly (van der Meer 2015). Cybercriminals are able to take advantage of the rapid rate of technological developments by exploiting vulnerabilities and security gaps in cyber-infrastructure.

Storing data on externally-hosted web services (e.g., cloud storage) potentially exposes Canadian businesses to cyber security risks (Bigo et al. 2012). In 2017, about one-third (31%) of businesses stored confidential business information on the Internet, such as information relating to their inventory or financial statements and 30% of businesses stored confidential information about their customers, suppliers or partners. Despite this, over half (54%) of businesses that used cloud storage did not employ their own data protection and control security measures such as encryption or rights management. This issue was more prevalent among small businesses (59%) in comparison to large businesses (20%). In some cases, these types of security protections may have been provided to the business by the cloud service provider.

There were also some noteworthy sectoral differences in 2017 with almost 63% of businesses in the oil and gas extraction sector[4] reported storing confidential business information on the Internet as opposed to hospitals[5] of which only 15% stored such information online.

The business sectors most likely to store confidential information about their customers, suppliers or partners on the Internet in 2017 included news syndicates, libraries and archives, Internet publishing and broadcasting and web search portals[6] (67%); natural gas distribution[7] (65%) and banking institutions (excluding investment banking)[8] (61%). Managing information in this way may have eventual consequences for some businesses as cybercriminals continue to advance ways to breach the storage of personal and financial data of customers (Bigo et al. 2012).

Two-thirds of businesses allow their employees to use personal devices for business purposes

Another possible doorway to cyber security attacks for businesses are through their employees who may use personal devices for business purposes. Vulnerabilities from personal devices could potentially spill over and compromise the business network, and vice-versa (Office of the Privacy Commissioner of Canada 2015).

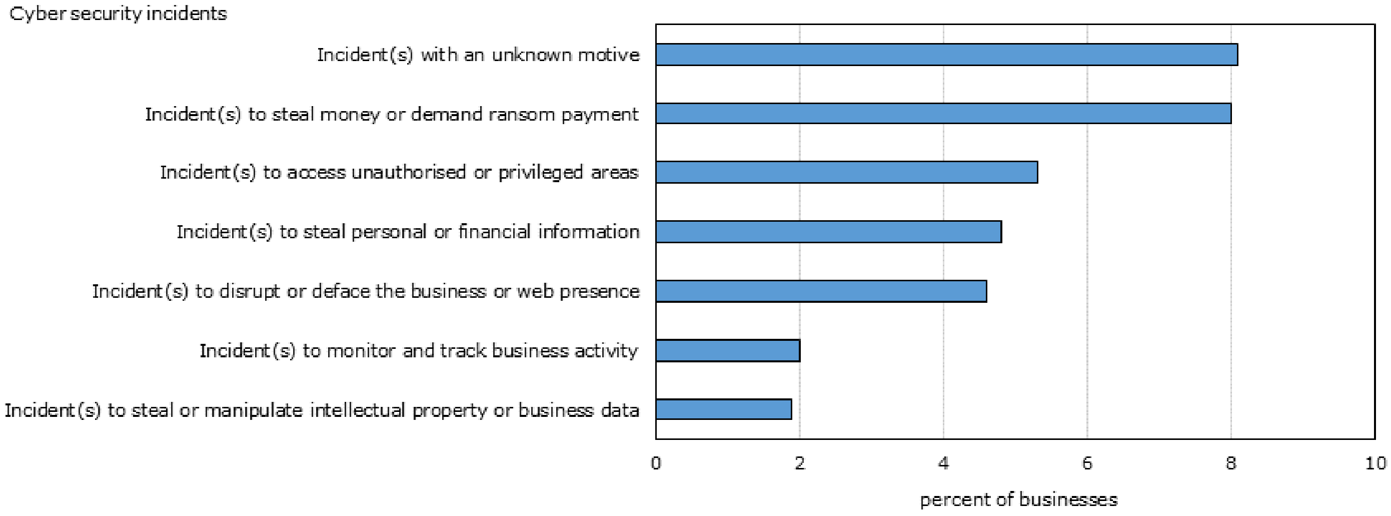
Two-thirds (66%) of businesses allowed their employees to use personal devices for business-related activities in 2017, which was generally consistent across different business sizes. However, the majority (64%) of small businesses (10 to 49 employees) did not have any security measures in place to manage the use of personal devices in comparison to 46% of medium-sized businesses (50 to 249 employees) and 21% of large businesses (250 employees or more). As such, small businesses are likely more vulnerable to cybercrime as they adopt technologies and services without implementing adequate security measures.

Just over one-fifth of Canadian businesses experienced impactful cyber security incidents

Just over one-fifth (21%) of Canadian businesses reported that they were impacted by cyber security incidents which affected their operations in 2017.[9] About 19% of small businesses reported being impacted compared to 28% of medium-sized businesses and 41% of large businesses.

Of those businesses that were impacted by cyber security incidents, 39% could not identify the motive of the attack, while 38% identified the motive as an attempt to steal money or demand a ransom payment. Just over one-quarter (26%) of businesses experienced incidents where perpetrators attempted to access unauthorized or privileged areas, while 23% experienced incidents where there was an attempt to steal personal or financial information (Chart 2).

Chart 2
Types of impactful cyber security incidents experienced, Canada, 2017



Source: Statistics Canada, Canadian Survey of Cyber Security and Cybercrime.

For all types of incidents, 65% of businesses reported that they believed an external party was responsible for the cyber security incidents. However, further information on these cybercriminals is often not known as the purpose of cybercrimes is generally to gain access to computers or computer networks while avoiding detection (van der Meer 2015).

Businesses that experienced an impactful incident in 2017 reported that the incidents were mostly perpetrated through scams and fraud (e.g., financial fraud, phishing) and malicious software (e.g., viruses, adware, ransomware).

More than half (54%) of impacted businesses reported that cyber security incidents prevented employees from carrying out day-to-day work, while close to one-third (30%) experienced additional repair or recovery costs. About 10% of businesses reported that they lost revenue, 6% reported that the incidents damaged the reputation of their business, 4% of businesses had to reimburse external parties or make a ransom payment and about 2% lost suppliers, customers or partners in 2017.

The majority (58%) of businesses that were impacted by cyber security incidents in 2017 experienced some downtime as a result of the incidents, while just over one-third (35%) of businesses reported that the incidents were minor and had minimal impact. On average, the total downtime for Canadian businesses in 2017 was 23 hours, and included mobile devices, desktops and networks.

When comparing risks taken on by businesses to incident rates, businesses that stored data on externally-hosted web services (e.g., cloud storage) were more likely than average to have experienced impactful incidents (26%). Similarly, businesses that allowed the use of personally-owned devices were also more likely than average to have experienced an impactful breach (24%). Overall, this was true across all business sizes.

In responding to impactful cyber security incidents, businesses were more likely to seek information or advice from an IT consultant or contractor (51%). Another 15% contacted a software or service vendor and about 12% of businesses spoke to their suppliers, customers or partners. Canadian businesses were also more likely to have sought information or advice through the internet community (e.g., forum, blog) (10%) than through police services (5%).

A greater number of businesses in critical infrastructure sectors experienced impactful incidents

Sectors which reported the highest level of cyber security incidents included banking institutions[8] (47%), universities[10] (46%) and pipeline transportation[11] (45%). Businesses in these sectors were mostly impacted by incidents to steal money or demand ransom payments in 2017.

Just over half (51%) of the banking institutions[8] that experienced any impactful cyber security incidents in 2017 reported that they lost revenue due to the incidents whereas the majority of universities (70%) and businesses in the pipeline transportation sector (76%) reported that their employees required additional time to respond to the incidents.

While Canadian businesses spent an average of $16,000 to recover from all impactful cyber security incidents in 2017, these average costs were substantially higher for businesses in critical infrastructure sectors. Businesses in the pipeline transportation sector spent $131,000, followed by businesses in the natural gas distribution sector ($118,000) and banking institutions[8] ($87,000). Comparatively, universities ($13,000) spent less than the average.

Increasingly, businesses in critical infrastructure sectors are being targeted by cybercriminals due to their widespread digital networks, interconnectedness, and significant value to the health, safety, security or economic well-being of Canadians. Businesses in these sectors manage assets and systems such as food supply chains, electricity grids, transportation infrastructure, communications infrastructure and public safety systems (see Gendron and Rudner 2012; Public Safety Canada 2009 for more details on emerging threats to critical infrastructures).

Text box 1
Cyber security measures and practices of businesses in the United Kingdom

The availability of comparable data on cyber security measures and practices of businesses is sparse as the majority of international surveys completed to date were not representative of overall businesses. These surveys had limitations due to small sample size, low response rates, and significant differences in the types of questions asked and the cyber security concepts used.

While data from the Canadian Survey of Cyber Security and Cybercrime and the United Kingdom’s (UK) Cyber Security Breach Survey, 2018 may have some differences, the two are most similar in content. As such, some comparisons are included here to understand whether the experience of Canadian businesses is similar to that of UK businesses (see Survey description section for a detailed description of these surveys).

Text box 1 — end
Cyber security measures and practices of businesses in the United Kingdom

Slightly more UK businesses experienced impactful cyber security incidents

About 23%[12] of UK businesses[13] experienced impactful cyber security incidents with over two-thirds (69%) of these businesses indicating that they needed new measures to address future attacks. The majority (60%) of impacted businesses in the UK reported that additional time was required by staff to deal with the incidents whereas almost one-third (32%) of Canadian businesses reported being impacted as such. Just over half of impacted businesses in the UK (51%) and Canada (54%) indicated that cyber security incidents or attacks stopped their staff from carrying out day-to-day work.

Businesses in both countries also indicated that they lost revenue or share value as a result of cyber security incidents (8% in the UK compared to 10% of Canadian businesses) and fewer businesses in Canada and the UK (6% in both) reported that the impactful incidents caused reputational damage.

While a direct comparison cannot be made on hours of downtime businesses experienced,[14] there is some evidence to suggest that cyber security incidents had similar effects on businesses in Canada and the UK. The majority (56%) of businesses in the UK that were impacted by breaches or attacks reported that it took them some amount of time to recover from their most disruptive attack, while similarly the majority (58%) of Canadian businesses reported experiencing some downtime as a result of an incident in 2017.

Similar to Canada, UK businesses who held personal data of customers were more likely than average to have had an impactful cyber security incident (27%) and those businesses that allowed the use of personally-owned devices also reported higher than average incidents (27%).

UK businesses spent on average $5,100 to recover from cyber security incidents with large and medium-sized businesses spending the most on recovery ($27,000 versus $37,000).[15]

One in ten Canadian businesses impacted by cyber security incidents reported the incidents to a police service

About 10% of Canadian businesses impacted by cyber security incidents reported the incidents to a police service in 2017. By far, banking institutions[8] were the most likely to report an impactful incident to a police service (60%) followed by a quarter (25%) of businesses in the electric power generation, transmission and distribution sector[16] and 24% of businesses in the pipeline transportation sector.

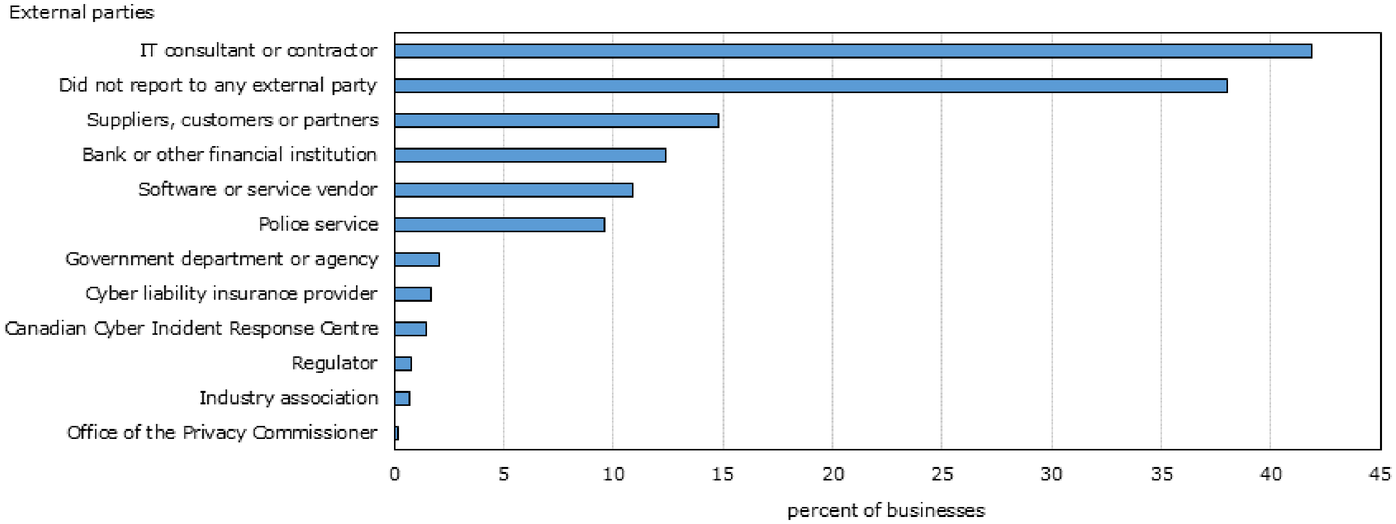
Such higher rates of reporting among certain types of businesses can be partly attributed to the partnerships between the Government of Canada and the owners and operators of critical infrastructures in these sectors. These partnerships are in place to prevent, respond to and recover from disruptions of critical infrastructures (Public Safety Canada 2009).

Over half (53%) of the businesses that were impacted by incidents and did not report them to a police service indicated that it was because the incidents were resolved internally. More than one-third (35%) of businesses did not report incidents because they were resolved through IT consultants or contractors, while 29% did not report the incidents to police services because they considered the impact to be too minor.

Over a quarter (26%) of impacted businesses did not think of contacting a police service and about 13% did not think that the perpetrator would be convicted or adequately punished. A few (4%) businesses found the reporting process too complicated or unclear or were unsatisfied with the response from the police service in the past (2%).

Impacted businesses also reported cyber security incidents to their suppliers, customers or partners (15%), bank or other financial institution (12%) and software or service vendors (11%) (Chart 3). Very few (1%) businesses reported incidents to the Canadian Cyber Incident Response Centre (CCIRC). However, reporting to CCIRC was higher among businesses in critical infrastructure sectors. These included banking institutions[8] (52%), businesses in the electric power generation, transmission and distribution sector (22%) and universities (18%).

Chart 3
External parties to which impactful incidents were reported, Canada, 2017



Source: Statistics Canada, Canadian Survey of Cyber Security and Cybercrime.

More than one-third (38%) of businesses did not report impactful cyber security incidents to any external party. This was partly attributable to the lack of reporting to other government departments or agencies (2%) or the Office of the Privacy Commissioner (less than one percent). However, reporting to the Office of the Privacy Commissioner is expected to increase over time as new regulations under the *Personal Information Protection and Electronic Documents Act* came into effect in November 2018, which made it mandatory for businesses to report breaches of security safeguards involving personal information (Office of the Privacy Commissioner of Canada 2018).

Additionally, 36% of businesses that were impacted by cyber security incidents indicated that incidents involving their organisation were reported to them by external parties. Businesses typically received these incident reports from their suppliers, customers or partners (17%) and IT consultants or contractors (15%). Almost half (47%) of these cyber security incidents were resolved internally and very few were reported to a police service (4%).

Text box 2
External reporting of cyber security incidents is lower among businesses in the United Kingdom than Canadian businesses

About 47% of businesses in the United Kingdom (UK) that were impacted by cyber breaches or attacks reported their most disruptive breach to external parties, while 64% of Canadian businesses impacted by cyber security incidents reported those incidents to external parties (including police services). Small (50%) and medium-sized businesses (43%) were more likely to report cyber security incidents to an external party than a large business (36%) in the UK. This was also true among businesses in Canada where 65% of medium-sized businesses and 64% of small businesses reported impactful incidents to an external party (including police services) in comparison to 53% of large businesses. In both countries, the differences in reporting practices by size of business is largely attributed to a greater percentage of small and medium-sized businesses reporting the incidents to their external IT consultant or contractor.

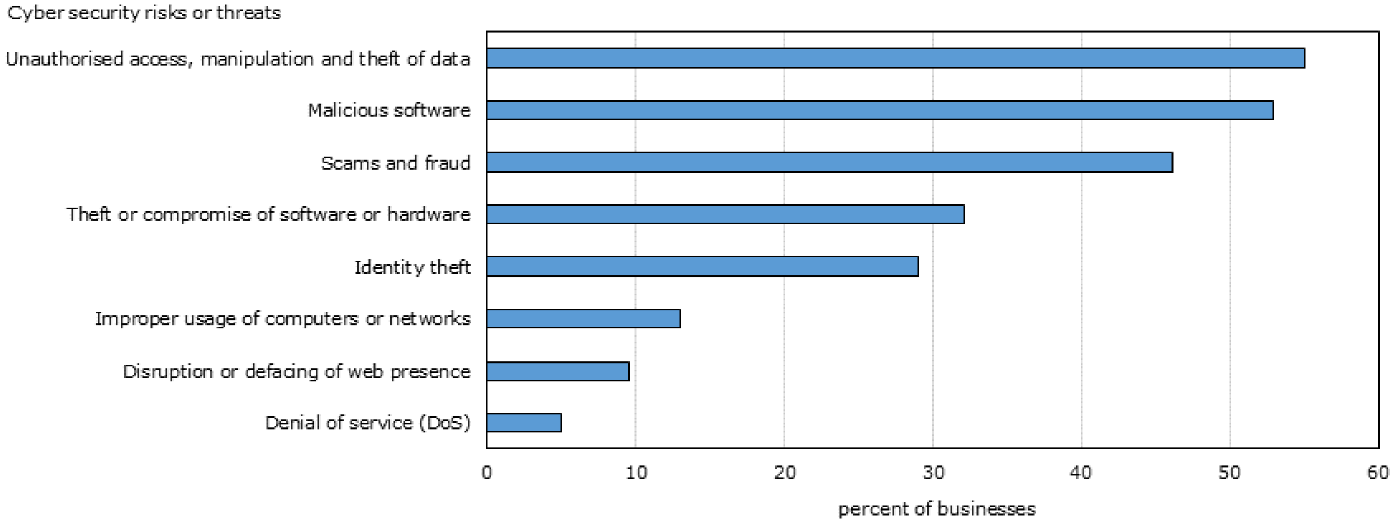
Of those businesses in the UK that were impacted by cyber breaches or attacks and reported their most disruptive breach to external parties, 39% reported these incidents to an outsourced cyber security provider, 16% reported them to a police service, 11% reported them to their internet service provider, and 10% of businesses reported them to a bank, building society or credit card company. Very few (5%) of these UK businesses reported their cyber security incidents to their clients or customers and even fewer (3%) reported it to their suppliers.

In most cases (57%), cyber security incidents experienced by UK businesses were identified by internal business staff, contractors or volunteers. However, about 6% of businesses in the UK were notified by their customers about a cyber security incident that impacted their organization.

Majority of Canadian businesses concerned about their vulnerability to cybercrime

The majority (85%) of Canadian businesses reported during the 2017 Canadian Survey of Cyber Security and Cybercrime that they were concerned about their vulnerability to future cyber security risks and threats, with 8% of businesses indicating that they were extremely concerned. Of those businesses that indicated that they were concerned about future cyber security threats, 60% indicated that unauthorized access, manipulation and theft of data would have a detrimental impact on their business. Over half (56%) of businesses reported that exploits from malicious software (e.g., viruses, adware, ransomware) would be damaging and about 47% of businesses reported that negative consequences would emerge from scams and fraud (e.g., financial fraud, phishing) (Chart 4).

Chart 4
Cyber security risks or threats that would have the most detrimental impact, Canada, 2017



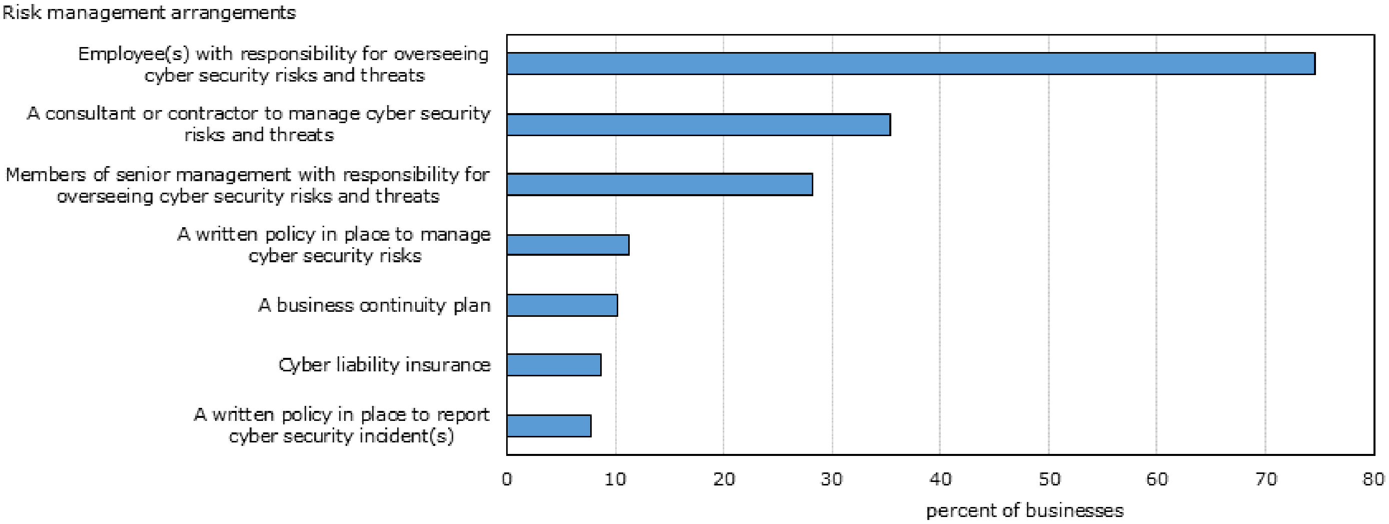
Source: Statistics Canada, Canadian Survey of Cyber Security and Cybercrime.

Even with such concerns, only 28% of businesses reported that members of senior management had the responsibility for overseeing cyber security risks and threats. This differed by size of business, with 52% of large businesses reporting that senior management had responsibility for overseeing cyber security risks and threats and about 26% of small businesses reporting such senior management involvement.

Certain industries were more likely to have senior managers oversee cyber security risks and threats. These included businesses in the computer systems design and related services sector[17] (69%), electric power generation, transmission and distribution sector (68%) and data processing, hosting and related services sector[18] (67%).

Over half (58%) of all businesses reported that senior managers were given updates on actions taken regarding cyber security, but very few (6%) businesses had tools for senior management to track cyber security issues. Lack of senior management involvement is also reflected in the fact that most (83%) businesses did not inform their senior managers about actions taken regarding cyber security after a cyber security incident had occurred. This may be explained by the fact that very few (8%) businesses had a written policy in place to report cyber security incidents. Additionally, few businesses had a written policy to manage cyber security risks (11%) or a continuity plan for when a cyber threat, vulnerability or risk was identified (10%) (Chart 5).

Chart 5
Types of risk management arrangements used, Canada, 2017



Source: Statistics Canada, Canadian Survey of Cyber Security and Cybercrime.

The lack of written policies and senior management involvement pose a serious risk to Canadian businesses as inadequate measures to safeguard privacy and data protection increase the potential for cybercrime. The limited use of these elements are also contrary to the advice provided by the Canadian Centre for Cyber Security, which recommends to businesses that senior management involvement in risk mitigation is essential in helping reinforce proper user behaviour and reduce vulnerabilities through appropriate security controls (Canadian Centre for Cyber Security 2018).

Canadian businesses spent an average of $78,000 on prevention and detection

The vast majority (94%) of businesses in Canada had some level of expenditure to prevent or detect cyber security incidents in 2017. On average, Canadian businesses spent $78,000 on implementing such measures. This was mainly driven by the average expenditure of large businesses ($922,000) and medium-sized businesses ($108,000). Small businesses reported spending an average of $44,000.

Businesses in the pipeline transportation sector spent the most on average ($2.2 million) on prevention and detection measures followed by $1.2 million by businesses in the natural gas distribution sector and $1.1 million by banking institutions.[8]

Across all businesses, the total average expenditure on employee salary for the prevention and detection of cyber security incidents was $40,000. Businesses further spent an average of $32,000 on other professional, scientific and technical services and $20,000 on hiring IT consultants or contractors in 2017.[19]

For large businesses, the amounts spent on such measures were vastly different. The average expenditure on hiring professional, scientific and technical services was $327,000, while total average salaries of employees for the prevention and detection of cybercrime was $305,000. This was followed by an average expenditure of $202,000 on IT consultants or contractors.

Over two-thirds (68%) of businesses reported that one of their motivations to spend time or money on preventing cybercrime was to protect personal information of employees, suppliers, customers or partners. About 41% reported that it was to prevent fraud and theft and about 31% of businesses indicated that expenditures on cyber security measures were to ensure continuity of business operations.

Text box 3
Fewer businesses in the United Kingdom spent money on cyber security compared to Canadian businesses

About two-thirds (66%) of businesses in the United Kingdom (UK) had some level of spending on cyber security, while in Canada this proportion was much larger. Spending levels in the UK were notably higher in certain sectors like in Canada, with businesses in the finance or insurance sector spending an average of $30,000. Businesses in the information or communications sector spent $24,000 on average, followed by businesses in the education sector spending an average of $14,000. These investments were largely driven by similar motives to Canadian businesses.

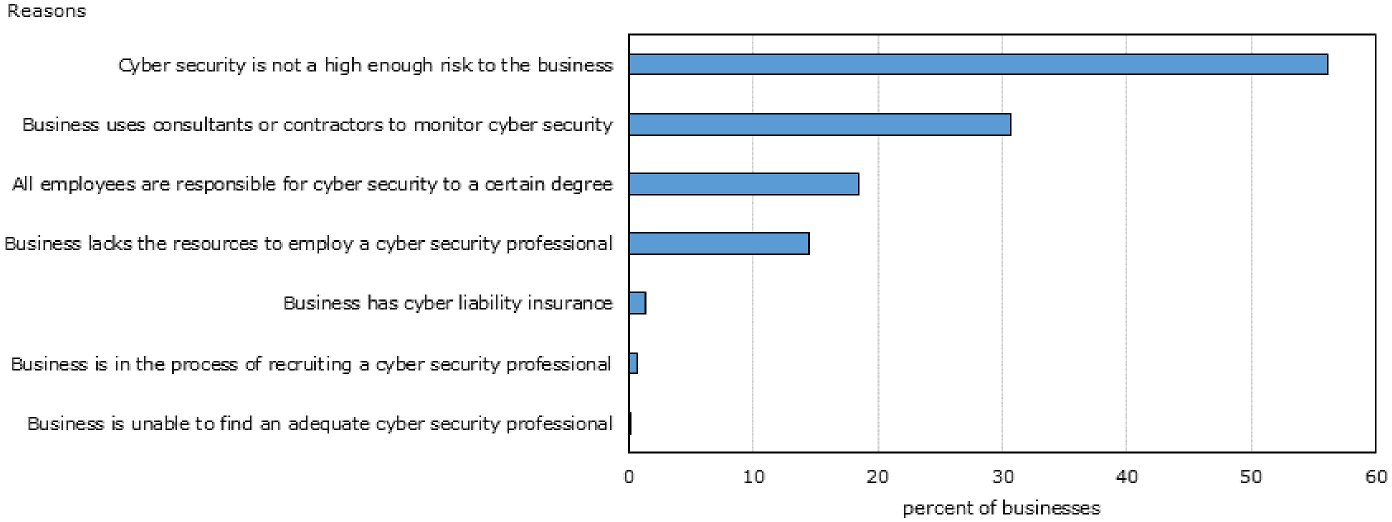
Majority of Canadian businesses had employees primarily responsible for cyber security

The majority of large (91%), medium-sized (83%) and small (72%) businesses in Canada reported having employees primarily responsible for the overall cyber security of their business in 2017.

Two-thirds (67%) of businesses, regardless of size, reported having at least one to five employees that were primarily responsible for cyber security. One-quarter (24%) of large businesses reported having more than five employees primarily responsible for cyber security compared with 9% of medium-sized businesses.

Among the 26% of businesses that did not have any employees primarily responsible for cyber security, more than half (56%) indicated that cyber security was not a high enough risk to their business and almost one-third (31%) indicated that they used consultants or contractors to monitor their networks. Of note, nearly 19% of businesses reported that all employees were responsible for cyber security to a certain degree and about 15% indicated that the business lacked the resources to employ a cyber security professional (Chart 6).

Chart 6
Main reasons for not having any employees primarily responsible for cyber security, Canada, 2017



Source: Statistics Canada, Canadian Survey of Cyber Security and Cybercrime.

Slightly over half (51%) of businesses shared general cyber security practices through email, bulletin boards or information sessions with their employees. These general practices often provided information on recognizing and avoiding email scams, the importance of password complexity and safe web browsing practices.

About 19% of businesses provided formal training to develop or upgrade their cyber security-related skills. Such training was provided almost equally among IT personnel and other employees in the business. Large businesses (59%) were most likely to provide training to their employees, while 32% of medium-sized and 16% of small businesses did so. On average, Canadian businesses spent $12,000 over the course of the year providing cyber security training to their employees, suppliers, customers or partners.

Additionally, the use of consultants or contractors to manage cyber security risks and threats was also quite prevalent. About 45% of medium-sized businesses used the services of consultants and contractors in comparison to 38% of large businesses and 33% of small businesses. The use of such services was commonly reported among businesses in the legal services sector[20] (72%).

Text box 4
Businesses in the United Kingdom were more likely to outsource cyber security responsibilities

Businesses in the United Kingdom (UK) were more likely to outsource the management of their cyber security (49%) than to have staff whose role included information security or governance (35%). Like Canadian businesses, medium-sized businesses in the UK were more likely to have outsourced their cyber security management practices (64%) compared to small and large businesses. The use of such external services was predominately used by businesses in the finance or insurance sector (73%).

Similarly, having at least one staff responsible for cyber security was more common among large businesses (76%) in comparison to medium-sized (62%) or small businesses (39%). UK sectors which were the least likely to have staff with cyber security responsibility included construction (22%) and food or hospitality (21%). In Canada, these sectors were food and beverage stores[21] (53%) and gasoline stations[22] (58%) in 2017.

There was also little variation between the two countries when it comes to cyber security training provided to staff. Among UK businesses, about 20% provided training to their staff through internal or external programs in comparison to 19% of businesses in Canada that provided such training.

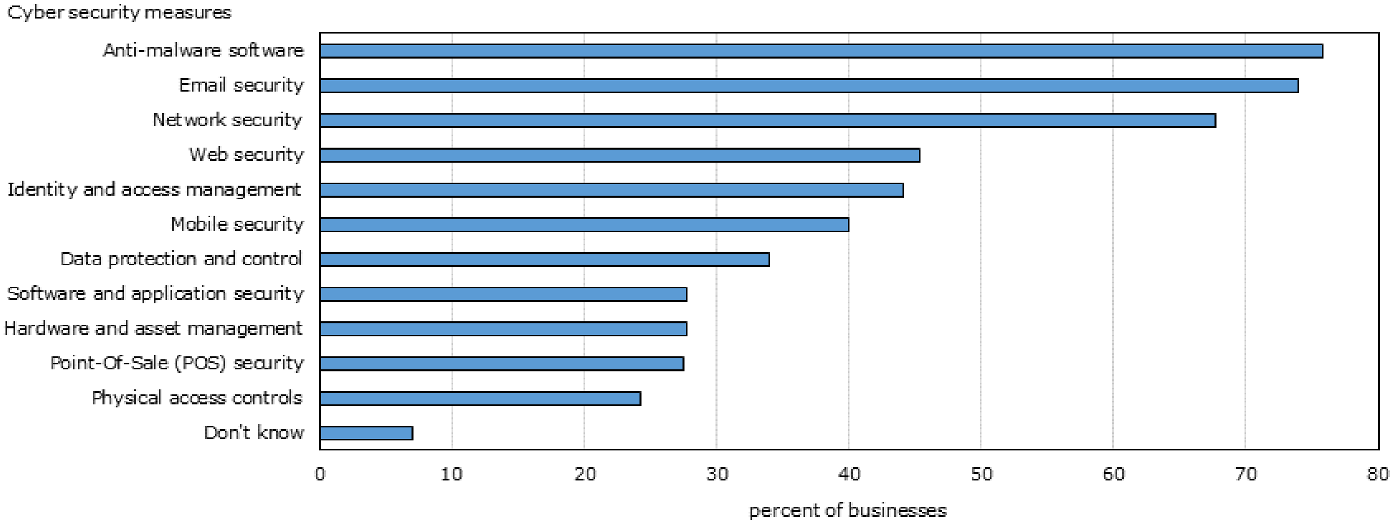
Use of cyber security measures has grown since 2013, with anti-malware software in high use

Very few (5%) Canadian businesses reported not having any cyber security measures to protect themselves, their customers and their partners in 2017. Over three-quarters (76%) reported that they had anti-malware software to protect against viruses, spyware, ransomware and other similar attacks, which is about the same percentage of businesses that reported using such software in 2013 (Statistics Canada 2013c).

The use of other cyber security measures has dramatically increased however. In 2017, the majority of businesses employed email security (74%) and network security (68%), while in 2013 about 53% of businesses reported using spam filters and 62% of businesses used a firewall.

Close to half (45%) of businesses employed web security such as website restrictions and 44% used identity and access management measures in 2017 in comparison to 13% of businesses that used web-filtering software and 19% of businesses that used authentication hardware or software for internal or external users in 2013 (Statistics Canada 2013c) (Chart 7).

Chart 7
Commonly employed cyber security measures, Canada, 2017



Source: Statistics Canada, Canadian Survey of Cyber Security and Cybercrime.

Approximately one-third (29%) of Canadian businesses were required to implement cyber security measures by their suppliers, customers, partners or regulators in 2017. These requirements were more common among banking institutions[8] (81%), health and personal care stores[23] (79%) and businesses in the pipeline transportation sector (67%).

In addition to the cyber security measures in place, over half (58%) of the businesses undertook activities to identify cyber security risks in 2017. A vast majority (93%) of large businesses undertook at least one activity to identify cyber security risks in comparison to 78% of medium-sized businesses and 54% of small businesses.

Large businesses were more likely to report using specialized external services to assess their cyber security risks compared with other business sizes, with 45% hiring an external party to conduct a penetration test of their security, 37% having their systems completely audited and 33% of businesses obtaining a formal risk assessment of their cyber security practices.

Of those businesses that undertook activities to identify cyber security risks, most (85%) monitored their network and business systems, while 38% monitored their employee's behaviours. Overall, these types of cyber security assessments were more common among businesses in the electric power generation, transmission and distribution sector (97%) and banking institutions[8] (96%).

Just over half (52%) of large businesses conducted such risk assessments on a scheduled basis. Meanwhile, 59% of small businesses and 56% of medium-sized businesses conducted assessments irregularly.

Some Canadian businesses also opted for additional security measures in 2017 with almost one-quarter (24%) of large businesses indicating that they had cyber liability insurance to protect against cyber security risks and threats, compared with 14% of medium-sized businesses and 7% of small businesses. This was more common among businesses in the natural gas distribution sector (54%); data processing, hosting and related services sector (50%) and banking institutions[8] (48%). Businesses in these sectors may be more inclined to purchase cyber liability insurance as they are considered to be high-value targets.

On average, Canadian businesses spent $14,000 over the course of the year on cyber liability insurance. The majority of insurance policies included coverage from direct loses from an attack or intrusion (82%), business interruption (72%), restoration expenses (71%) and third-party liability and financial losses (66%).

Text box 5
More businesses in the United Kingdom employ anti-malware software, network security and identity and access management protocols than Canadian businesses

The vast majority (92%) of businesses in the United Kingdom (UK) reported that they had rules or controls to apply software updates when they were available and about 90% had up-to-date anti-malware protection. A greater number of businesses in the UK also employed network security (89% had a firewall) and identity and access management protocols (78% restricted IT administrator and access rights to specific users) than Canadian counterparts.

Roughly the same percentage of businesses (38%) monitored user activity in Canada and the UK and about 12% of UK businesses required their suppliers to meet minimum cyber security standards.

Similar to Canadian businesses, more than half (56%) of all businesses in the UK undertook some action to identify cyber security risks to their organization. Most (89%) large businesses in the UK conducted one or more actions such as conducting a formal risk assessment or having an audit of their systems performed by an internal or external party.

The adoption of cyber security insurance policy was also similar among UK businesses and Canadian businesses (9%). Large (24%) and medium-sized (19%) businesses in the UK were more likely to have purchased these policies, along with businesses in the finance or insurance sector (20%).

Summary

Just over one-fifth (21%) of Canadian businesses reported that they were impacted by cyber security incidents which affected their operations in 2017. Of those businesses that were able to identify the motive of the attacks, 38% experienced an attempt to steal money or demand a ransom payment. Over one-quarter (26%) of businesses experienced incidents where perpetrators attempted to access unauthorized or privileged areas, while 23% experienced incidents where there was an attempt to steal personal or financial information.

Certain industries were more likely to be impacted by cyber security incidents in 2017, including banking institutions[8] (47%), universities (46%) and businesses in the pipeline transportation sector (45%).

More than one-third (38%) of businesses did not report an impactful cyber security incident to any external party. Of those businesses that did report, about 42% reported it to their IT consultant or contractor and 15% of businesses reported the incident to their suppliers, customers or partners. Few (10%) businesses reported the cyber security incidents to the police services in 2017.

On average, Canadian businesses spent $78,000 to prevent and detect cyber security incidents in 2017. This was mainly driven by the average expenditure of large businesses ($922,000) and medium-sized businesses ($108,000). Small businesses reported spending an average of $44,000.

Very few (5%) Canadian businesses reported not having any form of cyber security measures to protect themselves, their customers and their partners in 2017. About 74% of businesses had employees primarily responsible for the cyber security of their business, while 31% indicated that they solely used consultants or contractors to monitor their networks.

Key terminology and definitions

Adware: Software that automatically displays or downloads advertising material (often unwanted) when a user is online.

Anti-malware: A type of software program designed to prevent, detect and remediate malicious programming on individual computing devices and IT systems.

Authentication hardware or software: Hardware or software used to authenticate or verify a user’s identity prior to being granted access or approving a transaction request.

Business continuity plan: A strategy that recognizes threats and risks facing a company, with the purpose to ensure that users and assets are protected and able to function in the event of a major issue.

Cloud computing: The ability to access all required software, data and resources via a computer network instead of the traditional model where these are stored locally on a user’s computer.

Cloud storage: Data is stored, accessed and shared through remote servers accessed from the Internet.

Denial of Service (DoS): A cyber-attack where the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet.

Downtime: A time during which a machine, domain or service is not productive, as during repair, malfunction, or maintenance. This can lead to reduced activity or inactivity of a user or a business.

E-commerce platforms: A software technology solution that allows a business to build and host a digital storefront soliciting a specific set of products or services.

Email security: All the security measures used to filter and manage the emails a user receives and secure access to their account (e.g., spam filters, email scans).

Encryption: Converting information into a code that can only be read by authorized users who have been provided with the necessary (and usually unique) "key" and special software so that they can reverse the process (e.g., decryption) and use the information.

Financial fraud: An attempt by a criminal to obtain, through fraudulent means, a victim's bank account number, online banking login information and/or credit card information with the intent to steal money.

Firewall: A hardware and/or software device on a computer that controls the access between a private network and a public network like the Internet. A firewall is designed to provide protection by stopping unauthorized access to the computer or network.

Identity and access management measures: Measures implemented on a computer network to manage the access of particular user accounts and maintain their security (e.g., password complexity rules, restrictions based on user accounts).

Internet-connected 'smart' devices: Electronic devices that can connect to each other and the Internet through a network. These devices are designed to automatically send and receive information from the Internet on a constant basis.

Mobile security: The protection of smartphones, tablets, laptops and other portable computing devices, and the networks they connect to, from threats and vulnerabilities associated with wireless computing.

Network security: The protection of the access to files and directories in a computer network against hacking, misuse and unauthorized changes to the system.

Penetration testing: An authorized simulated attack on a computer system that looks for security weaknesses, potentially gaining access to the system's features and data. The test can help determine whether the IT infrastructure is vulnerable to attack, if the defenses are sufficient, and which defenses (if any) the test defeated.

Phishing: A specific kind of spam targeting one or more specific user(s) while pretending to be a legitimate message, with the intent of defrauding the recipient(s).

Physical access controls: Controls to allow authorized users access to a place or other sources (e.g., turnstiles, key pass, passwords).

Point-Of-Sale security: A secure software to record when goods or services are sold to customers.

Ransomware: A type of malware that restricts access to a user's computer or files and displays a message that demands payment in order for the restriction to be removed.

Rights management: Restrictions to create and consume protected content such as emails and documents.

Social media: Social networking websites or applications like Facebook, Twitter and LinkedIn. Businesses use these to reach potential customers, build stronger relationships and for marketing or other professional purposes.

Spam filters: A set of rules to screen email that has been sent without the permission or request of the user it has been sent to.

Spyware: Software that collects information about a user without their knowledge. It often comes in the form of a 'free' download and is installed automatically with or without consent.

Virus: Malicious computer programs that are often sent as an email attachment or a download with the intent to infect a computer or network. It often contains spam, provide criminals with access to the computer or network and disable the security settings.

Voice over internet protocol (VOIP): Routing of voice conversations over the Internet. This is distinct from a telephone call, which is made from a home or office phone which goes through the Public Switched Telephone Network.

Web-filtering software: Software which prevents users from accessing certain Internet addresses in order to protect the user's device and/or computer network against attacks.

Web security: A branch of computer security specifically related to the Internet, often involving browser security but also network security on a more general level as it applies to other applications or operating systems on a whole. Its objective is to establish rules and measures to use against attacks over the Internet.

Web services: A service that is made available from a business's Web server for Web users or other Web-connected programs. A prevalent example of a Web service is storage management and customer relationship management application.

Survey description

Canadian Survey of Cyber Security and Cybercrime

The Canadian Survey of Cyber Security and Cybercrime (CSoCC) was conducted for the first time in 2018 on behalf of Public Safety Canada. The purpose of the survey was to collect data on the impact of cybercrime on Canadian businesses and their activities to mitigate the effects.

The survey was launched to benchmark and monitor the rapidly evolving environment surrounding cyber security and cybercrime. As an emerging issue, data of this type had not been collected by the Government of Canada previously on this scale.

Data for the survey were collected from January to April 2018 through an electronic questionnaire. The target population included businesses with Canadian operations and with 10 or more employees, across all sectors, with the exception of public administration. Businesses with operations in any Canadian province or territory were in scope for this survey.

The survey was sent to the IT manager or senior member of staff that was the most knowledgeable on the business' cyber security practices. Respondents were asked to report details of cyber security incidents that impacted their business in 2017. The response rate was 86%, yielding a sample of 10,794 businesses.

Data limitations

Since businesses are not always aware of cyber security incidents that have impacted them or are unwilling to report certain incidents, survey results may have been affected by underreporting bias.

Businesses were only asked to report on incidents that impacted them on the Canadian Survey of Cyber Security and Cybercrime. Therefore, incidents that businesses deemed not to be impactful are not captured in these data.

Cyber Security Breaches Survey 2018

The Cyber Security Breaches Survey 2018 conducted by United Kingdom's (UK) Department for Digital, Culture, Media and Sport provides insight into the behaviours and practices of UK businesses and charities as they respond to cyber security threats. The survey was divided into two parts, the first being a random probability telephone survey of 1,519 UK businesses and 569 UK registered charities. This was conducted from October 9, 2017 to December 14, 2017. The second portion was a follow up interview with 50 organizations that participated in the survey, as well as higher education institutions. This portion of the study was undertaken in January and February of 2018.

For the purposes of this paper, the information derived from the first portion of the UK study was compared to the results of the Canadian Survey of Cyber Security and Cybercrime (CSoCC) where appropriate. This comparison was made with the results stemming from the UK study on businesses alone as charities were out of scope for CSoCC. Variance estimation and significance testing were not done on the analysis of the two datasets. For further information on the methodology and sampling strategy of the UK survey, see Department for Digital, Culture, Media and Sport 2018.

References

Bank of Canada. 2017. "Annual exchange rates." *Bank of Canada*. December 29. (accessed December 11, 2018).

Bigo, D., G. Boulet, C. Bowden, S. Carrera, J. Jeandesboz and A. Scherrer. 2012. *Fighting Cyber Crime and Protecting Privacy in the Cloud*. European Parliament Committee on Civil Liberties, Justice and Home Affairs. PE no. 462.509.

Canadian Centre for Cyber Security. 2018. *Top 10 IT Security Actions to Protect Internet Connected Networks and Information*. ISTM no. 10.189. (accessed December 28, 2018).

Department for Digital, Culture, Media and Sport. 2018. Cyber Security Breaches Survey, 2018. [data collection]. UK Data Service. SN no. 8406.

Gendron, A. and Rudner, M. 2012. *Assessing Cyber Threats to Canadian Infrastructure*. Study. Canadian Security Intelligence Service. (accessed December 28, 2018).

Office of the Privacy Commissioner of Canada. 2018. *New Data Breach Reporting Requirements Come Into Force This Week*. News Release. Office of the Privacy Commission of Canada. (accessed November 30, 2018).

Office of the Privacy Commissioner of Canada, Office of the Information and Privacy Commissioner of British Columbia and Office of the Information and Privacy Commissioner of Alberta. 2015. *Is a Bring Your Own Device (BYOD) Program the Right Choice for Your Organization?* Office of the Privacy Commissioner of Canada. (accessed December 21, 2018).

Public Safety Canada. 2009. *National Strategy for Critical Infrastructure*. ISBN no. 978-1-100-11248-0. (accessed December 27, 2018).

Statistics Canada. 2018a. *Uniform Crime Reporting Survey*. Surveys and Statistical Programs. Canadian Centre for Justice Statistics. Record number 3302. (accessed December 12, 2018).

Statistics Canada. 2018b. *The General Social Survey: An Overview*. Surveys and Statistical Programs. Statistics Canada Catalogue no. 89F0115X. (accessed December 12, 2018).

Statistics Canada. 2013a. *Enterprises with a Website by Industry and Size of Enterprise*. Table 22-10-0016-01. (accessed November 28, 2018).

Statistics Canada. 2013b. *Website Features by Industry and Size of Enterprise.* Table 22-10-0017-01. (accessed November 28, 2018).

Statistics Canada. 2013c. *Enterprises Identifying Information and Communications Technology (ICT) Security Practices, by Industry and Size of Enterprise.* Table 22-10-0032-01. (accessed November 28, 2018).

van der Meer, S. 2015. “Enhancing International Cyber Security.” *Security & Human Rights*. Vol. 26, nos. 2 to 4. p. 193-205.

Notes

1. Statistics Canada also collects data on cybercrime through the Uniform Crime Reporting Survey. This is an annual survey of police-reported crime that was modified in 2004 to allow police to flag any criminal incident as “cyber”, meaning report it as any criminal act as outlined in Canada’s *Criminal Code* where information and communication technology (ICT) is the target of the offence, or whereby ICT is integral and vital in the commission of the offence.

In addition, as part of the annual crime statistics reporting, Statistics Canada reports on crimes that are inherently cyber such as non-consensual sharing of intimate images, luring a child via computer, child pornography, etc. See Statistics Canada 2018a for more details.

Social issues that are often associated with cybercrime such as cyberbullying and cyberstalking are captured through the victimization module of the General Social Survey. “The data are an important complement to administrative data on police-reported crime, as they capture information that does not come to the attention of the police and is therefore not counted in official crime rates.” (Statistics Canada 2018b).

2. For Canadian businesses, analysis by size splits the population into small businesses (10 to 49 employees), medium businesses (50 to 249 employees) and large businesses (250 employees or more).

3. Data on social media usage is not directly comparable between 2017 and 2013 as respondents were asked in the Canadian Survey of Cyber Security and Cybercrime (CSoCC) whether the business had a social media account whereas in the Survey of Digital Technology and Internet Use (SDTIU), respondents with websites were asked whether they integrated the business’s social media accounts to their business’s website.

More importantly, 2013 data from SDTIU includes businesses that had 0 or more employees whereas CSoCC surveyed businesses with 10 or more employees. As such, due to the divergent methodologies between surveys, comparisons should be made cautiously.

4. This sector refers to North American Industry Classification System code 211 (Oil and gas extraction).

5. This sector refers to North American Industry Classification System code 622 (Hospitals).

6. This sector refers to North American Industry Classification System code 519 (Other information services).

7. This sector refers to North American Industry Classification System code 2212 (Natural gas distribution).

8. This sector comprises North American Industry Classification System (NAICS) code 521 (Monetary authorities – central bank) and NAICS code 522 (Credit intermediation and related activities). The sector excludes investment banking.

9. In the Canadian Survey of Cyber Security and Cybercrime, respondents were asked about the types of incidents that impacted their business operations. Respondents had the flexibility to define and identify what constituted as an impactful incident on their business operations. Data on incidents which respondents deemed not to have an impact on business operations were not collected.

10. This sector refers to North American Industry Classification System code 6113 (Universities).

11. This sector refers to North American Industry Classification System code 486 (Pipeline transportation).

12. The percentage of the overall business population in the United Kingdom (UK) that was impacted by cyber security incidents was calculated using the microdata from the Cyber Security Breaches Survey 2018. The calculation was restricted to include only those businesses that experienced cyber security breaches or attacks and reported being impacted by such incidents. This was done to compare the results from the UK survey to the Canadian Survey of Cyber Security and Cybercrime. This value differs from the UK Statistical Release, which indicated that 43% of UK businesses experienced cyber security breaches or attacks. The value presented in the UK Statistical Release included those businesses that experienced an attack or breach which were not impactful to their operations.

13. The business population for the United Kingdom was split into the following size groups: micro businesses (1 to 9 employees), small businesses (10 to 49 employees), medium businesses (50 to 249 employees) and large businesses (250 employees or more).

14. These data are not directly comparable as the United Kingdom's Cyber Security Breaches Survey 2018 measured the recovery time from a cyber security incident, whereas the Canadian Survey of Cyber Security and Cybercrime measured the downtime businesses experienced from an incident.

15. Calculation of average costs for businesses in the United Kingdom includes values of "0" whereas costs reported for Canadian businesses excludes these values. As such, comparisons of costs between the two countries must be made cautiously.

All costs reported in the UK's Cyber Security Breaches Survey 2018 were reported in UK pound sterling. For ease of comparison, these costs have been converted to the Canadian dollar at the 2017 annual average exchange rate published by the Bank of Canada. The exchange rate was 1.6720, expressed as one unit of the UK pound sterling converted into Canadian dollars.

16. This sector refers to North American Industry Classification System code 2211 (Electric power generation, transmission, and distribution).

17. This sector refers to North American Industry Classification System code 5415 (Computer systems design and related services).

18. This sector refers to North American Industry Classification System code 518 (Data processing, hosting, and related services).

19. Values of "0" were excluded from all dollar figure calculations of Canadian businesses. As such, every dollar figure reported for Canadian businesses uses a slightly different population and they cannot be summed to a total average expenditure.

20. This sector refers to North American Industry Classification System code 5411 (Legal services).

21. This sector refers to North American Industry Classification System code 445 (Food and beverage stores).

22. This sector refers to North American Industry Classification System code 447 (Gasoline stations).

23. This sector refers to North American Industry Classification System code 446 (Health and personal care stores).