Impact of cybercrime on Canadian businesses, 2017

Released at 8:30 a.m. Eastern time in The Daily, Monday, October 15, 2018

The Canadian Survey of Cyber Security and Cybercrime was conducted for the first time to measure the impact of cybercrime on Canadian businesses. This release coincides with Cyber Security Awareness Month, which is an internationally recognized campaign held each October to inform the public of the importance of cyber security.

Canadian businesses report spending $14 billion on cyber security

Canadian businesses reported spending $14 billion to prevent, detect and recover from cyber security incidents in 2017, which represented less than 1% of their total revenues. Approximately $8 billion was spent on salaries for employees, consultants and contractors who worked on cyber security, while $4 billion was invested in cyber security software and related hardware. Several other prevention and recovery measures accounted for the remaining $2 billion of the total expenditure.

Annual average expenditures on cyber security differed greatly based on size of business in 2017. Large businesses (250 employees or more) spent $948,000, medium-sized businesses (50 to 249 employees) spent $113,000 and small businesses (10 to 49 employees) spent $46,000.

Just over one-fifth of Canadian businesses are impacted by a cyber security incident

In 2017, just over one-fifth (21%) of Canadian businesses reported that they were impacted by a cyber security incident which affected their operations. Large businesses (41%) were more than twice as likely as small businesses (19%) to have identified an impactful incident.

Of those businesses that were impacted by a cyber security incident, 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% faced an incident where there was an attempt to steal personal or financial information.

More than half (54%) of impacted businesses reported that cyber security incidents prevented employees from carrying out day-to-day work, while 53% reported that incidents prevented the use of resources or services (for example, desktop computers or email). Close to one-third (30%) of businesses faced additional repair or recovery costs, 10% lost revenue and 4% reported that they had to reimburse external parties or make a ransom payment in 2017.

Over half (58%) of businesses experienced some downtime as a result of an incident. On average, the total downtime for businesses in 2017 was 23 hours, and included mobile devices, desktops and networks.

Businesses in certain sectors were more likely to be impacted by cyber security incidents. Banking institutions (excluding investment banking) (47%), universities (46%) and businesses in the pipeline transportation subsector (45%) reported the highest level of incidents.

For all types of incidents, 65% of businesses reported that they believed an external party was responsible for the cyber security incident, as opposed to an internal employee, supplier, customer, partner or unknown actor.

The vast majority of Canadian businesses have some form of cyber security in place

Nearly all Canadian businesses (95%) employed some form of cyber security to protect themselves, their customers and their partners in 2017. However, even for the most commonly reported protective measures, usage was not universal. A number of businesses did not use anti-malware software (24%), email security (26%) and network security (32%), such as firewalls. Among large firms, the use of these security measures was nearly universal.

While two-thirds (66%) of businesses allowed their employees to use personally owned devices to carry out business-related activities, 47% of these businesses had security measures in place to manage these devices.

Approximately one-third (29%) of 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 (excluding investment banking) (81%), health and personal care stores (79%) and businesses in the pipeline transportation subsector (67%).

Almost one-quarter (24%) of large businesses indicated 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. For a majority of the policies, coverage included direct losses from an attack or intrusion (82%), business interruption (72%), restoration expenses (71%) and third-party liability and financial losses (66%).

Almost three-quarters of Canadian businesses have employees responsible for cyber security

In 2017, 74% of businesses in Canada had employees primarily responsible for the cyber security of their business, led by large-sized (91%) and medium-sized (83%) businesses.

Just over two-thirds (67%) of businesses in Canada, regardless of size, reported having one to five employees who were primarily responsible for cyber security. Almost one-quarter (24%) of large businesses reported having more than five employees primarily responsible for cyber security, compared with 9% for medium-sized businesses.

In 2017, among the 26% of businesses that reported not having any employees primarily responsible for cyber security, 56% indicated that cyber security was not a high enough risk to their business, while 31% indicated that they used consultants or contractors to monitor their networks.

Slightly over half (51%) of businesses shared general cyber security practices through email, bulletin boards or information sessions with their employees, while 19% provided formal training to develop or upgrade their cyber security-related skills. 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.

Few Canadian businesses have a written policy to manage or report cyber security incidents

In 2017, 13% of businesses had a written policy in place to manage or report cyber security incidents. However, certain industries surpassed the average, including banking institutions (excluding investment banking) (66%), and those in the pipeline transportation (55%) and rail transportation (55%) subsectors.

Among the 58% of businesses that undertook any activities to identify cyber security risks in 2017, most (85%) monitored their network and business systems, while 38% monitored their employees' behaviours.

The vast majority of large businesses (93%) undertook at least one activity to identify cyber security risks. These 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 IT systems completely audited and 33% obtaining a formal risk assessment of their cyber security practices.

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

Over one-quarter (28%) of businesses reported having senior managers oversee cyber security risks and threats, and 89% of these businesses reported that they updated senior managers on actions taken regarding cyber security.

Most Canadian businesses do not report cyber security incidents to law enforcement agencies

About 10% of businesses impacted by a cyber security incident reported the incident to a police service in 2017. Of those that did report, 79% reported an incident to steal money or demand a ransom payment and 56% reported an incident related to the theft of personal or financial information.

Just over half (53%) of the businesses that were impacted by incidents did not report them to a police service because the incidents were resolved internally. Meanwhile, 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.

Chat session

The public is invited to chat with an expert on this topic on Wednesday October 17, 2018, from 1:30 to 2:30 p.m., Eastern Time.

Note to readers

Canadian businesses continue to rapidly embrace the Internet and digital technologies, which 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.

The 2017 Canadian Survey of Cyber Security and Cybercrime, the first of its kind in Canada, aims to address some of these data gaps by providing a snapshot of the current threat environment in a manner not previously possible, providing new and current insights into the behaviour of Canadian businesses as they meet the cyber security challenges of a changing world.

Data for the survey were collected from January to April 2018. The target population included businesses with Canadian operations and with 10 or more employees, across all sectors, with the exception of public administration. The final sample size was 12,597 businesses and the response rate was 86%.

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. Therefore, incidents that businesses deemed not to be impactful are not captured in these data.

Average dollar fiqures were calculated excluding responses of zero dollars.

The category referenced in this article as banking institutions (excluding investment banking) can be found in tables 22-10-0001-01, 22-10-0056-01 and 22-10-0076-01 to 22-10-0079-01, under the label monetary authorities - central bank, credit intermediation and related activities. This category comprises North American Industry Classification System (NAICS) code 521 (Monetary authorities - central bank) and NAICS code 522 (Credit intermediation and related activities).

Available tables: 22-10-0001-01, 22-10-0056-01 and 22-10-0076-01 to 22-10-0079-01 .

Definitions, data sources and methods: survey number 5244.

The infographic "Cybercrime and Canadian businesses, 2017," which is part of *Statistics Canada — Infographics* (**11-627-M**), and an interactive dashboard "Cyber Security and Cybercrime in Canada, 2017," which is part of *Statistics Canada — Data Visualization Product* (**71-607-X**), are now available.

For more information, or to enquire about the concepts, methods or data quality of this release, contact us (toll-free 1-800-263-1136; 514-283-8300; **STATCAN.infostats-infostats.STATCAN@canada.ca**) or Media Relations (613-951-4636; **STATCAN.mediahotline-ligneinfomedias.STATCAN@canada.ca**).