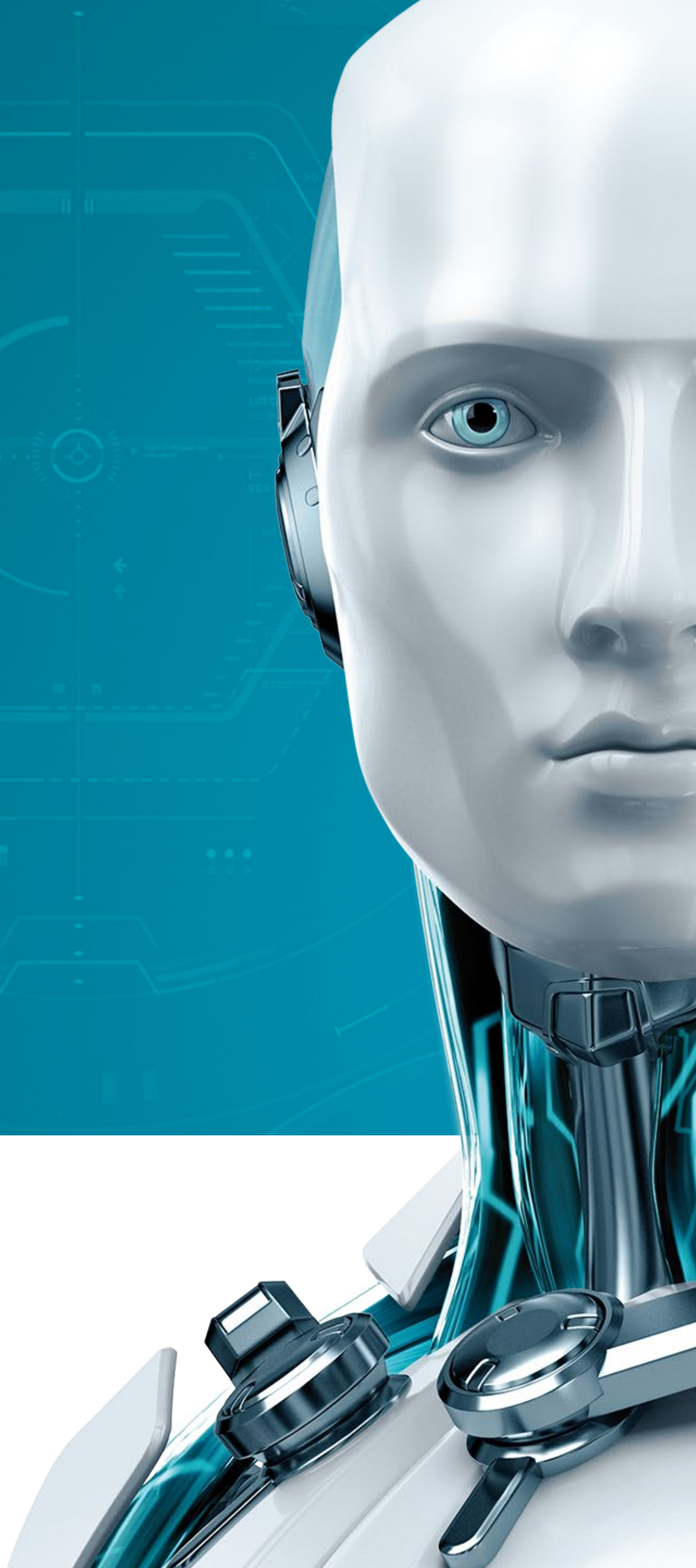
ENJOY SAFER TECHNOLOGY™

The State of SMB Cybersecurity in Canada 2016

Independently conducted by Ipsos
Sponsored by ESET Canada

Publication Date: October 2016



PART 1: Introduction

Client records, accounting history, trade secrets, personal information — what would happen to your business if it was all stolen or you suddenly couldn't access it? For many small and medium-sized businesses (SMBs), the issue of cybersecurity is often eclipsed by other business priorities that hoard the company's operating budget. SMB owners often believe that they are not a target for hackers because they don't harbour enough valuable information, and thus allocating funds and man hours to cybersecurity falls off the radar.

The reality is that SMBs handle the same types of sensitive data that cybercriminals target in larger organizations. SMBs aren't immune to cyberattacks – and far from it. Smaller businesses are often targeted as a way to get inside big businesses. Forbes reports that cyberattacks are costing businesses $400–$500 billion a year, and that does not include the majority of cyberattacks, most of which are not reported. There is a day to day business of cybercrime, of ransomware campaigns, of harvesting information by infecting machines. It is a very well developed business. And as your small business grows, it exposes itself to a wider audience and at the same time, naturally increases its attack surfaces.

This puts SMBs in a cybercrime sweet spot. Relative to consumers, SMBs have more digital assets and cash that is worth targeting via criminal hacking. Relative to enterprises, SMBs have fewer cybersecurity protections in place.

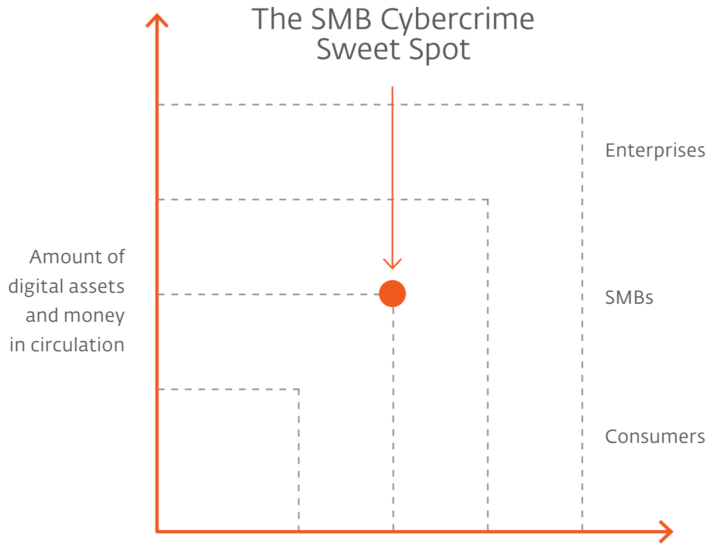
New Canadian research from Ipsos validates this. It shows that the risk of cyberattack spikes for Canadian SMBs once they reach $10 million in annual revenue, with one in four with annual revenue of $10–$24 million becoming victims, compared to only one in 10 firms with annual revenue under $10 million. Not that the latter have nothing to worrying about, far from it. For a start, many small firms are working hard to grow their revenues, but they might not be fully aware of the cybercrime risks inherent in such growth.

Making adequate financial provisions for dealing with increased cyber risks as your business grows is clearly a prudent strategy. However, it is not clear if Canadian SMBs are getting this message. For example, this Ipsos survey reveals a disconnect among employees regarding, on the one hand, their company's allocation of resources to cybersecurity, and on the other, confidence regarding their company's level of protection from attack. While seven in 10 Canadians employed at SMBs feel their company is devoting enough resources to the issue, only one third feel 'very confident' their company is safe from a cyberattack.

Sometimes this type of disconnect occurs when people are not fully aware of the threats that their organizations face from cyber criminals. For example, any organization that is serious about cybersecurity will perform a risk analysis to determine what digital assets are at risk and what level that risk is at. A company is underestimating its cyber risks if it is not aware that criminals can sell its customer data for good prices on black markets with little chance of arrest, or make money by renting out its hijacked servers for use in malicious activities.

The picture of Canadian SMB cybersecurity that emerges from this survey is of many good intentions and a broad awareness that cybercrime is a threat to the organization. For instance, 96% of Canadian SMB employees think that backing up company files is important, and 92% think having IT security software installed on all devices is an important IT security measure. A very encouraging 88% place a strong emphasis on “training on your company’s IT security procedures”. Yet, much work remains to be done. Only 43% of Canadian SMB employees feel confident that their business and its reputation could “survive and thrive” after a cyberattack. And only 40% say they are “very satisfied” with their company’s current IT security policies, procedures, and products.

With clear evidence that the risk of cyberattack increases with revenue growth, there is a definite need for Canadian SMBs to keep improving their awareness of threats and their ability to deflect them. There is always plenty of room to better align cyber policy, procedure, and product selection with the full range of current threats, because the threats are unlikely to diminish any time soon.


The SMB Cybercrime Sweet Spot
Amount of digital assets and money in circulation
Enterprises
SMBs
Consumers

PART 2: Key Findings

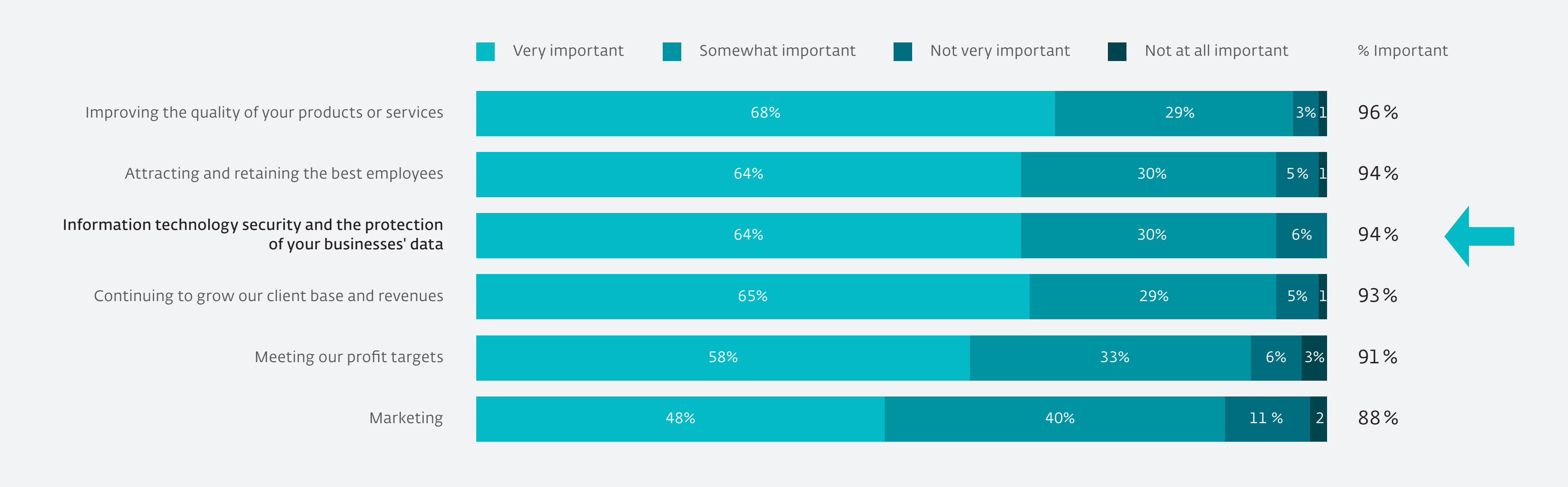
Small and medium-sized businesses (SMBs) in Canada are not immune to cyberattacks, with one in five (18%) employees of Canadian SMBs saying their workplace has been a victim of a cyberattack.

Cyberattacks are more likely to have occurred at Canadian SMBs with yearly revenue over $10 million. For instance, three in ten (29%) employees from businesses with a yearly revenue of $25–$99 million and one in four (24%) employees from businesses with a yearly revenue of either $10-$24 million or over $100 million indicated that they have been victims of a cyberattack.
This is compared to only one in ten companies in the $1-9 million (13%) or less than $1 million (12%) range indicating they have been a victim of a cyber-attack.

Further, more small-sized business employees say that they have never been victims of a cyber-attack (76%) compared to employees from medium-sized businesses (70%).

Given the prevalence of high-profile cyberattacks and leaks in the news media, it's perhaps not surprising that two in three (64%) employees say that it is very important their businesses participate in activities involving "information technology security and the protection of our businesses' data."

Q: How important do you view the following activities for your business?



Being Attacked

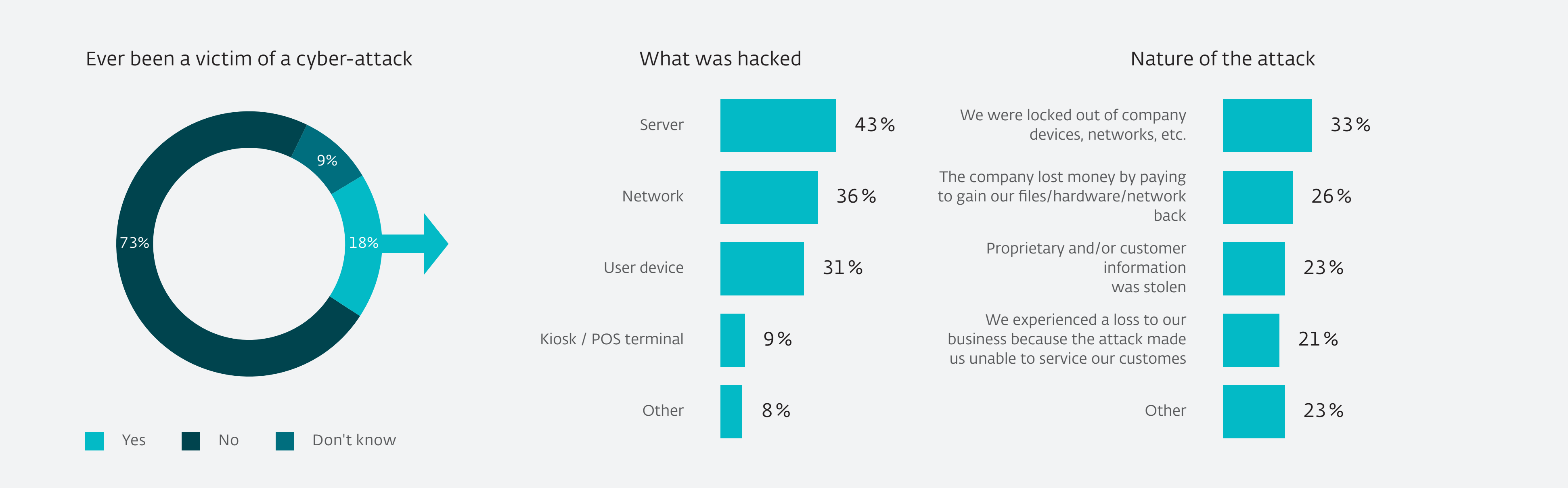
Among the two in ten (18%) employees whose company has been a victim of a cyber-attack, the most common device to have been hacked is the server (43%), followed by the network (36%), user device (31%), kiosk/point-of-sale terminal (9%) or some other type of attack (8%).

During the attack, one in three (33%) victims say that some employees were locked out of company devices, networks, etc. Two in ten victims say that their companies "lost money by paying to gain their files/hardware/networks back" (26%), "proprietary and/or customer information was stolen (23%) or they "experienced a loss to our business because the attack made us unable to service our customers" (21%). Slightly more than two in ten (23%) employees said the nature of the attack was something other than these options.

18% of companies has been victim of a cyber-attack

43% of it was via servers

Q: Has your organization ever been a victim of a cyber-attack?

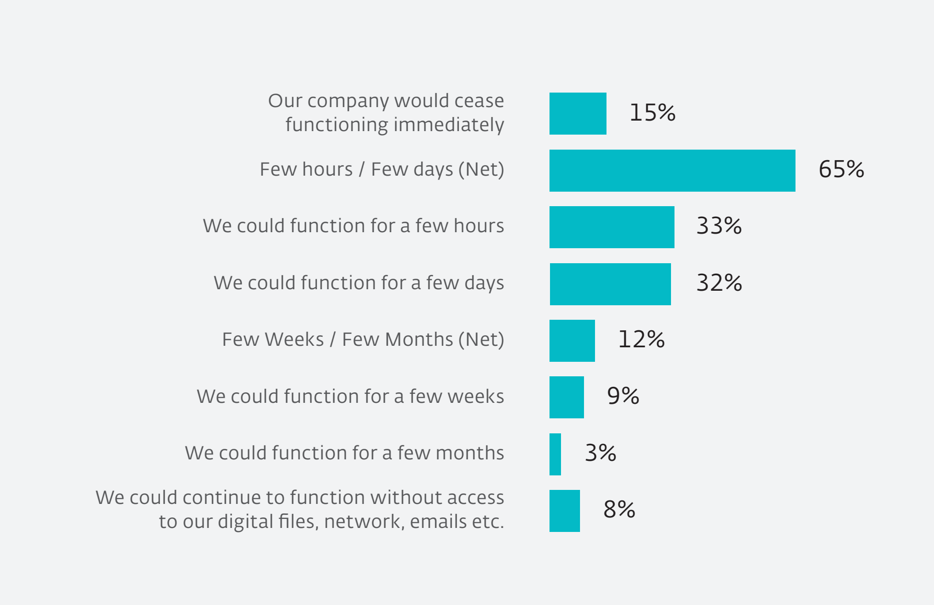


What is particularly concerning is that the majority of Canadian SMBs, which according to Statistics Canada make up 98% of the country's businesses, would be unable to function for more than a few days without access to their data. Sixty-five per cent of Canadian SMBs can only function for a few hours or days without access to their data, and a full 15% of Canadian SMBs would have to cease functioning immediately.

98% of the country's business would be unable to function more than a few days without access to their data

15% of Canadian SMBs would have to cease functioning immediately

Q: How long do you think your business could function without access to its digital files, the network, emails, etc?



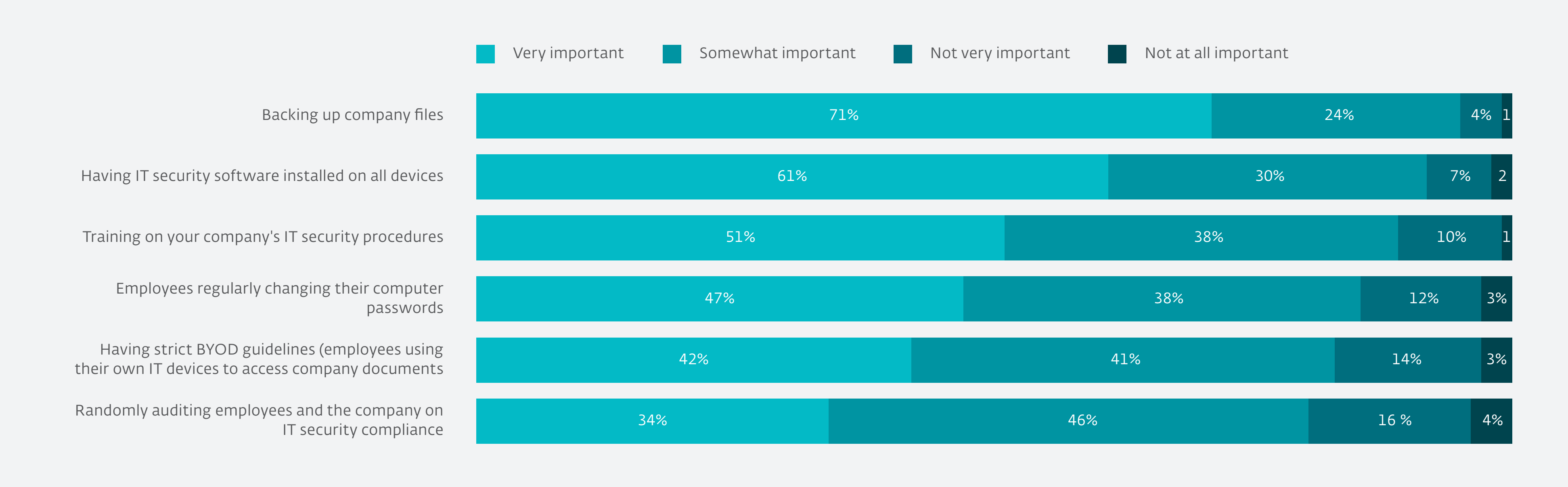
Importance of IT Policies, Procedures and Products

A majority of Canadian SMB employees believe it is important for their businesses to take action to protect and safeguard their business information. For instance, nine in ten employees think backing up company files (96%) and having IT security software installed on all devices (92%) are important IT security measures their organizations can take, followed by "training on your company's IT security procedures" (88%), employees regularly changing their computer passwords (86%), having strict BYOD guidelines on employees using their own IT devices to access company documents (83%), and randomly auditing employees and the company on IT security compliance (81%).

86%
employees regularly changing their computer passwords

61%
of all employees find very important to have IT security software installed on all devices

Q: How important do you think the following IT (information technology) policies, procedures or products are for your organization in protecting and safeguarding your business information?

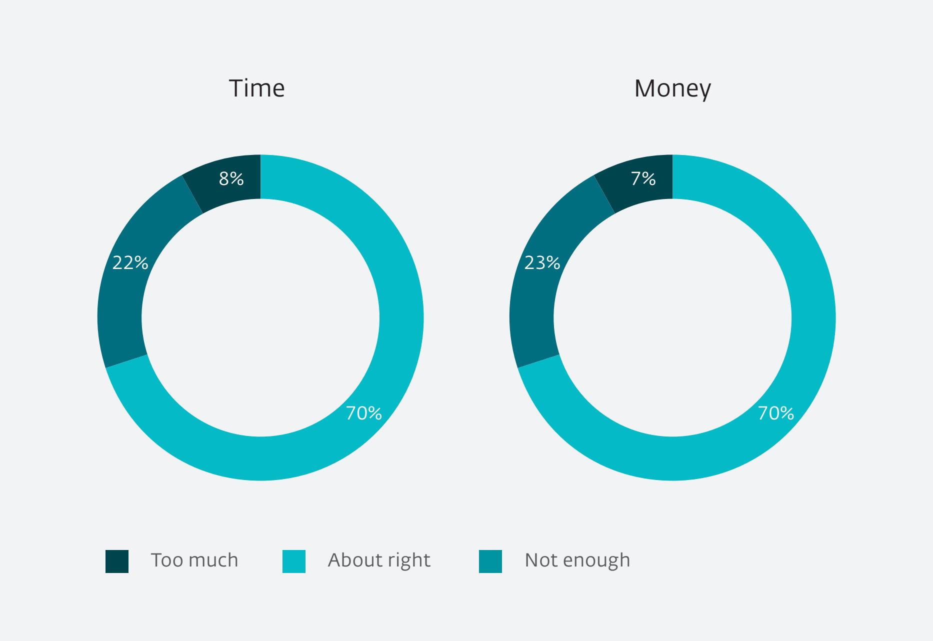


Are Canadian SMBs Doing Enough?

Only two in ten (22%) Canadian employees say that their organization is not spending enough time on IT security. Seven in ten (70%) say the amount of time spent on IT security is about right, and only one in ten (8%) say their organization is spending too much time.

When it comes to the amount of money organizations are spending on IT security, one in four (23%) employees say that their organization is not spending enough. Canadian employees' views on time tend to be the same as their views on money spent: seven in ten (70%) say the amount of money spent on IT is about right, and only one in ten (8%) believe their organization is spending too much money on IT security.

Q: Do you believe that the amount of time and money that your organization spends on IT security is: too much, about right, not enough?



That being said, when Canadian SMB employees were asked how confident they are that their business and its information would be safe from a cyberattack, only one in three (33%) of Canadian employees were "very confident" that their businesses would be safe. This means that more than half (67%) have some reservation about their company's ability to protect itself and its information if a cyberattack were to occur. Further, only two in five (40%) of employees are "very satisfied" with their company's current IT security policies, produces and products.

Being Prepared

Employees were asked how often their staff is given information, training or practice IT procedures to ensure IT security. Three in four (75%) say their staff backs up their files on an ongoing or monthly basis. Half (56%) say the staff at their organization uses their own IT devices to access company documents on an ongoing/monthly basis, while four in ten (42%) say staff change their computer passwords at this same frequency. Only one in three (34%) say that staff is trained on their company's IT security procedures on an ongoing/monthly basis, and a further one in three (32%) say the same about the frequency with which staff is audited on their IT security compliance.

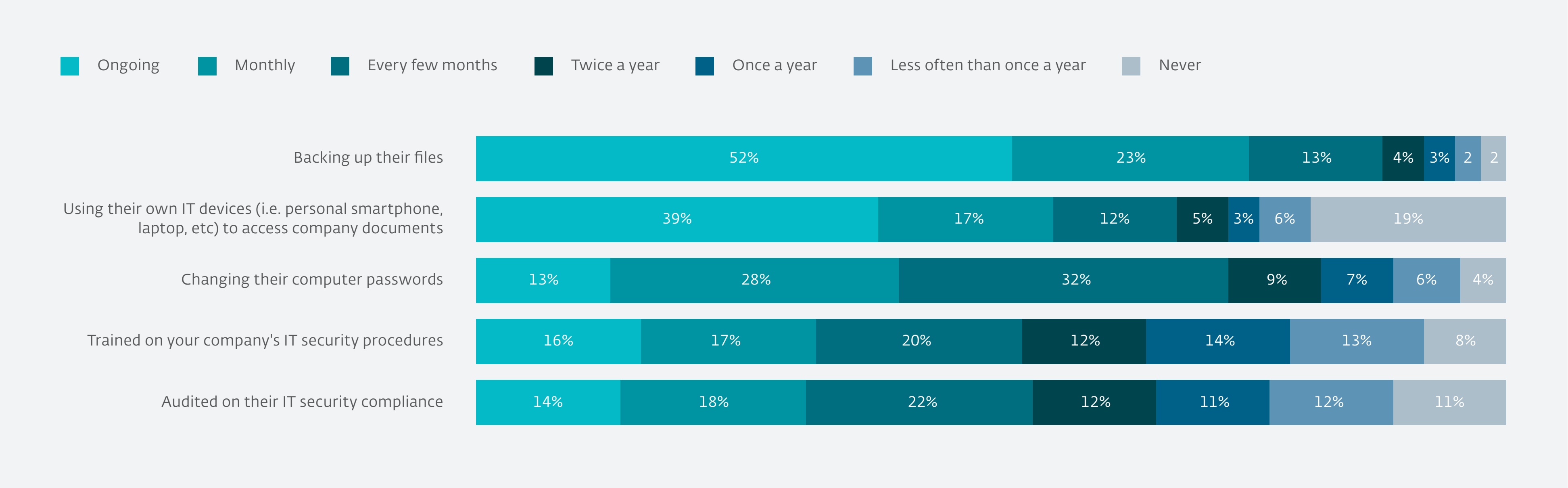
42%

of staff change their computer passwords on an ongoing/ monthly basis

34%

say that staff is trained on their company's IT security procedures on an ongoing/ monthly basis

Q: How often is your staff doing the following?

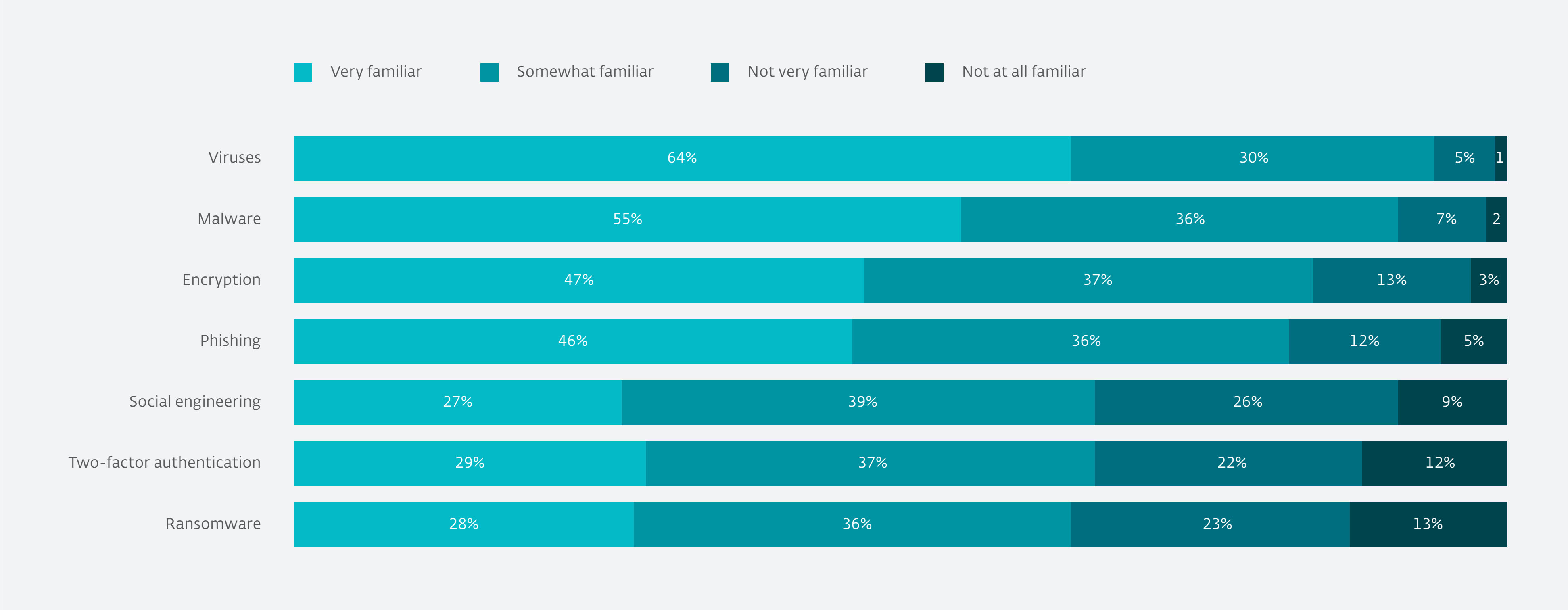


There seems to be a general awareness among Canadian SMB employees of terms dealing with IT security, however there is certainly room for improvement. With two exceptions, less than half of those surveyed describe themselves as being “very familiar” with the following terms: viruses (64% are very familiar), malware (55%), encryption (47%), phishing (46%), two-factor authentication (29%), ransomware (28%) and social engineering (27%).

64% of Canadian employees are familiar with term "viruses"

29% of Canadian employees are familiar with term "two-factor authentication"

Q: How familiar are you with the following terms?



PART 3: Five Things to Know About Protecting your Small or Medium-Sized Business

Cybersecurity for a small business can be a daunting task when you're strapped for time and resources, but there are plenty of resources available to help, including a variety of partners, advisors and vendors who can provide advice and solutions specific to your business needs. Here are five basic things you should know about protecting your business and its assets:

1 Threats to SMBs occur both inside and outside a business.
The two biggest threats inside a business are: data loss from user errors, and employees that steal or leak information like client lists. The two biggest threats outside of a business are: phishing/social engineering and ransomware. Phishing is when employees are tricked into revealing account credentials, whether banking, social media or other system logins via a malicious email or link. This can then be used to hijack data, resources and money. Ransomware is a type of malicious software (or malware) that holds files hostage until a ransom is paid. A study from ESET Canada in April 2016 showed that that 63% of Canadians are not, or don't know if they are, protecting themselves from ransomware.

2 One size solution does not fit all, but it is not as complicated as it sounds.
There is no magic solution that protects every type and size of business. Securing your business is as easy as looking at your potential areas for data loss, your potential points of entry, and then getting advice on the best ways to close those gaps. That being said, you can hire a managed serviced provider or a cloud provider to help you protect your business, but you cannot offload your security liability. You are ultimately the one responsible for any data or business loss.

3 SMBs need to continue to scale and upgrade their security services as their business grows, not just in terms of the number of devices they are protecting with antivirus, but also by consistently evaluating the security solutions that are specific to their evolving business practices.

As the nature of your business changes, (e.g. you add field reps, remote workers, or implement a "bring your own device" policy) your business's network gets more complicated and dispersed. For example, having employees who work on the road or at home means that accessing your network from around the world becomes necessary. But, with that comes the potential of your remote workers connecting to insecure Wi-Fi networks or losing their company devices, which could put your company, your credentials and your resources at risk.

4 Your employees are both your best asset and your weakest link.
Using your staff to fight cybercrime is not as daunting as it seems. Making your staff feel an integral part of the security of your business is an important aspect of a robust cybersecurity strategy. This can be done by regular education and auditing of employee behavior. Make sure your employees know the current threats and how they attack. It can make all the difference and prevent an employee from accidentally clicking that phishing link or visiting a compromised website.

5 There are a few basic security practices you can use to keep your business safe:
Require strong passwords or passphrases on all devices and require them to be changed frequently. Even better, implement strong two-factor authentication that requires a password AND a second confirmation, whether on a mobile device, or with a biometric like a fingerprint.

Additionally, you should be updating firmware and software as needed and not letting anything go unpatched if an update exists. Multi-layered security software is also a must. It should be installed on every endpoint and server. You should also be backing up your data regularly. In the event that you do fall victim to a cyberattack, or your files are locked up by ransomware, you'll be able to rest easy knowing that your essentials are backed up and easily accessible.

PART 4: Methodology

These key findings are a portion of an Ipsos poll conducted between August 22 and August 26, 2016, on behalf of ESET Canada. For this survey, a sample of 1,003 Canadian adults employed at small businesses (defined as companies with 5–99 employees) and medium businesses (defined as companies with 100 to less than 500 employees), who work in IT, are senior management or who have a broad knowledge of their company's IT policies and procedures from Ipsos' online panel was interviewed online.

Weighting was then employed to balance demographics to ensure that the sample's composition reflects that of the adult population according to Census data and to provide results intended to approximate the sample universe.
The precision of Ipsos online polls is measured using a credibility interval. In this case, the poll is accurate to within +/- 3.5 percentage points, 19 times out of 20, had all Canadian adults employed at small and medium businesses in these job functions been polled. The credibility interval will be wider among subsets of the population. All sample surveys and polls may be subject to other sources of error, including, but not limited to coverage error, and measurement error.

Contact

For more information about this study, please contact Sean Simpson, Vice President, Ipsos Public Affairs, at (416) 324-2002 or sean.simpson@ipsos.com.

Ipsos

Ipsos is Canada's market intelligence leader and the country's leading provider of public opinion research. With operations in eight cities, Ipsos employs more than 600 research professionals and support staff in Canada. The company has the biggest network of telephone call centres in Canada, as well as the largest pre-recruited household and on-line panels. Ipsos' Canadian marketing research and public affairs practices are staffed with seasoned research consultants with extensive industry-specific backgrounds, offering the premier suite of research vehicles in Canada—all of which provide clients with actionable and relevant information. Ipsos is an Ipsos company, a leading global survey-based market research group. To learn more, visit www.ipsos.ca.

ESET Canada

For over 25 years, ESET® has been developing industry-leading security software for businesses and consumers worldwide. With security solutions ranging from endpoint and mobile defense to encryption and two-factor authentication, ESET's high-performing, easy-to-use products give users and businesses the peace of mind to enjoy the full potential of their technology. ESET unobtrusively protects and monitors 24/7, updating defenses in real time to keep users safe and businesses running uninterrupted.

In 2015, ESET expanded into Toronto, Canada's largest technology hub, with a Canadian office to complement the existing ESET research office in Montreal and position ESET to better meet customer demand across Canada.

For more information, visit www.eset.com and check out the ESET blog at www.welivesecurity.com for more research and insights into today's cybersecurity trends and issues.

ESET business products can be sourced through a wide selection of reseller partner network throughout Canada and North America. Consumer products are available at Best Buy, Staples, London Drugs and online at www.eset.com.

If you would like to speak to an ESET representative to discuss security business requirements, or to request a custom business trial or technical demo, please contact us at (416) 637-1465 or james.chalmers@eset.ca to speak to the ESET Canada Director of Partner Sales and Alliances.