ENJOY SAFER TECHNOLOGY®

The State of SMB Cybersecurity in Canada 2017

Independently conducted by Ipsos
Sponsored by ESET Canada

Publication Date: September 2017

Contents

02
Part 1:
Introduction

04
Part 2:
Key findings

19
Part 3:
Tips to set your SMB business up for success

20
Part 4:
Methodology

Part 1: Introduction

Canadian employees of small and medium-sized businesses (SMBs) are fearful that their business will be unable to handle a cyber-attack. In fact, there is a general lack of confidence among employees when it comes to their organization's ability to keep the business and its information safe.

Rising concern among SMB employees

- Nearly half (45%) of employees believe that their business is at risk of a cyber security attack, 8% of whom say they perceive their organization to be significantly at risk. If an attack were to occur, a majority (74%) of employees are not confident that their organization would be able to keep their business and its information safe, leaving only one quarter (26%) of employees who are very confident, a 7-point drop from September 2016.
- Rising concern may be driven by the lack of knowledge, training and time employees feel is being spent on cyber security within their organization.
    - **35%** concerned with **lack of knowledge** among staff about how the organization could be attacked
    - **24%** concerned with **lack of knowledge** about how the organization is currently being protected
    - **24%** concerned with **lack of training** on the organization's cyber security procedures
    - **23%** concerned with **lack of time spent** on staying current with cyber security issues
    - **19%** concerned with **lack of investment** in cyber security protection systems for the organization

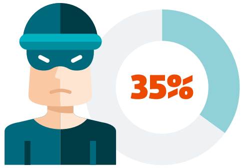
- However, while many are concerned with the lack of time and money spent on cyber security protection, investing more time and money into IT security is not among the most popular course of action.
- Less than two in ten (14%) employees say their organization does not spend enough, down 9 points, while eight in ten (79%) say they spend about the right amount, and 7% say they are spending too much money on IT security.
- When it comes to devoting time to the issue, only 14% of employees say their companies are not spending enough time on cyber security, whereas three in four (76%) believe they are spending the right amount of time, and one in ten (10%) claim they are spending too much time.
- In short, SMB employees believe their companies are investing just about the right amount of time and money in cyber security, and tend to be more concerned with the lack of training and knowledge they personally have on their organization's IT security policies, procedures, and products.

45%

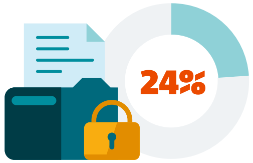
of employees believe that their business is at risk of a cyber security attack

8%

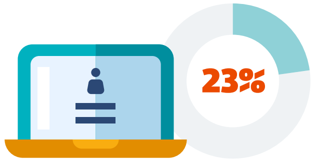
of whom say they perceive their organization to be significantly at risk



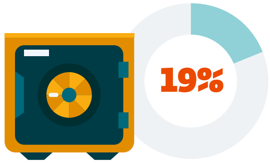
Don't know how their organization could be attacked.



Don't know how their organization is currently being protected.



Don't spend enough time on staying current with cybersecurity issues.



Don't spend enough in cybersecurity protection systems.

Part 2: Key findings

05 Important activities for your business

06 Protecting and safeguarding your business information

07 Staff and IT training

08 How often organizations update cyber security procedures

09 How often organizations update cyber security software

10 Current layers of cyber security in place protecting the business

11 Amount of time and money spent on IT security

12 Concerns about level of cyber security

13 Familiarity with IT terms

14 Confidence your business is safe from cyber-attacks

15 Time your business can function without digital files

16 Victim of a cyber-attack

17 What was hacked

18 Nature of the attack

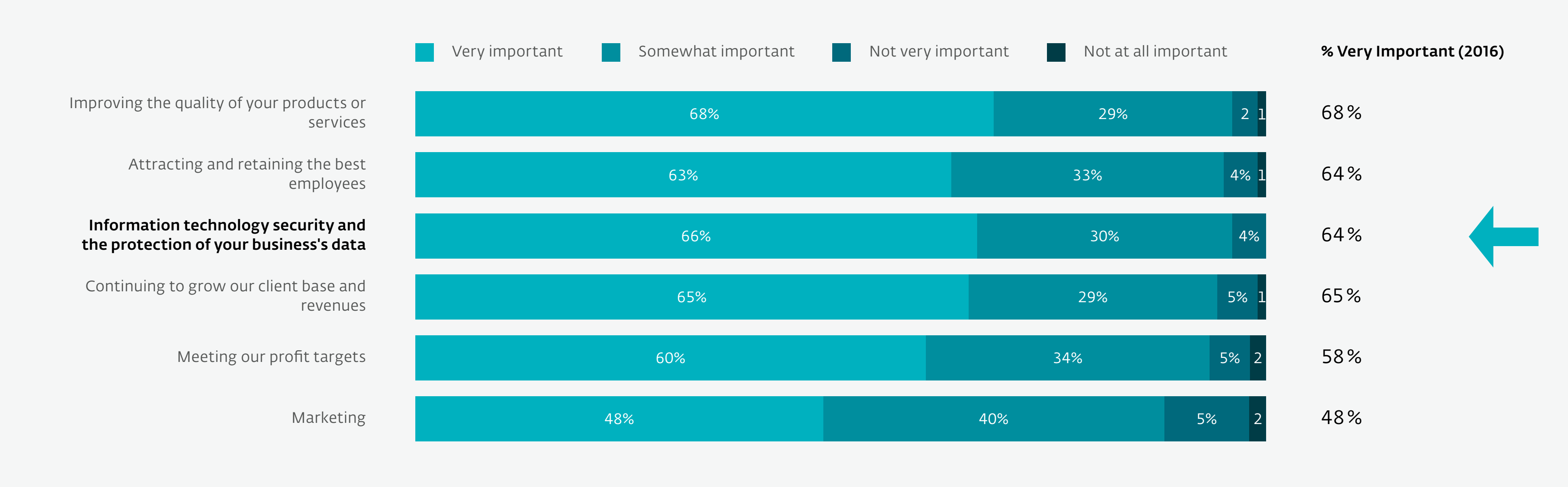
Important activities for your business

Two in three (66%, +2 pts) employees say it is very important that their business participates in activities involving information technology security and the protection of their business's data. The only other activity that is of more importance to employees is improving the quality of their business's products or services.

66%

of employees say that IT security is as important as improving their products or services (68%)

Q.1 How important do you view the following activities for your business?

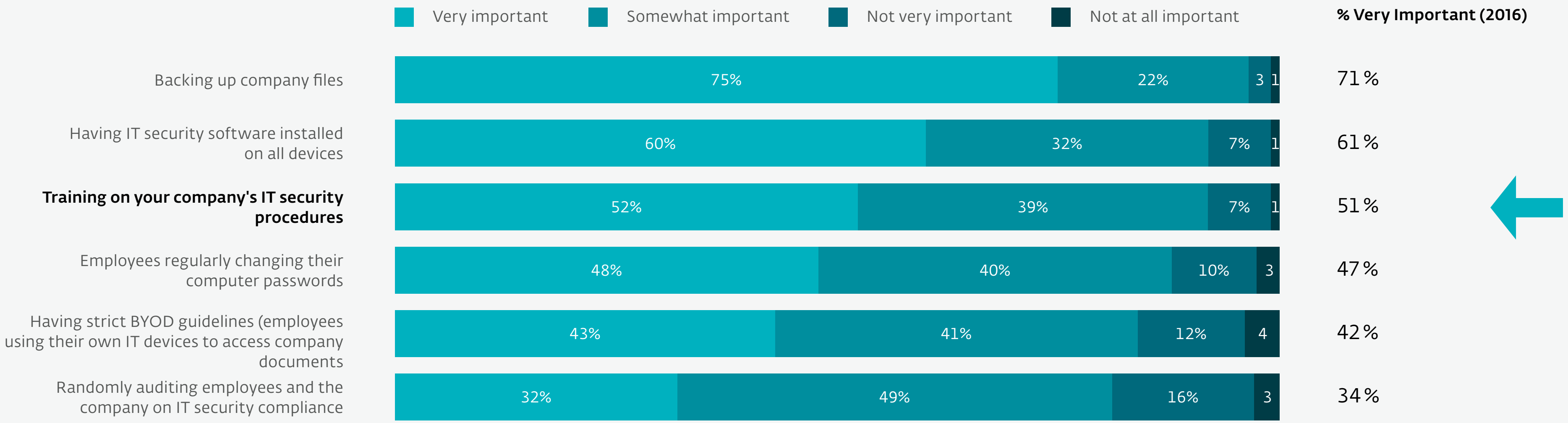


Base: All respondents 2016 (n=1003); 2017 (n=1003)

Protecting and safeguarding your business information

When it comes to protecting and safeguarding company information, a majority (75%) of employees say backing up company files is the most important protocol they can take, up 4 points. Having IT security software installed on all devices (60%), and engaging in training on company's IT security procedures (52%) are also seen as very important IT policies companies can invest in.

Q.2 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?

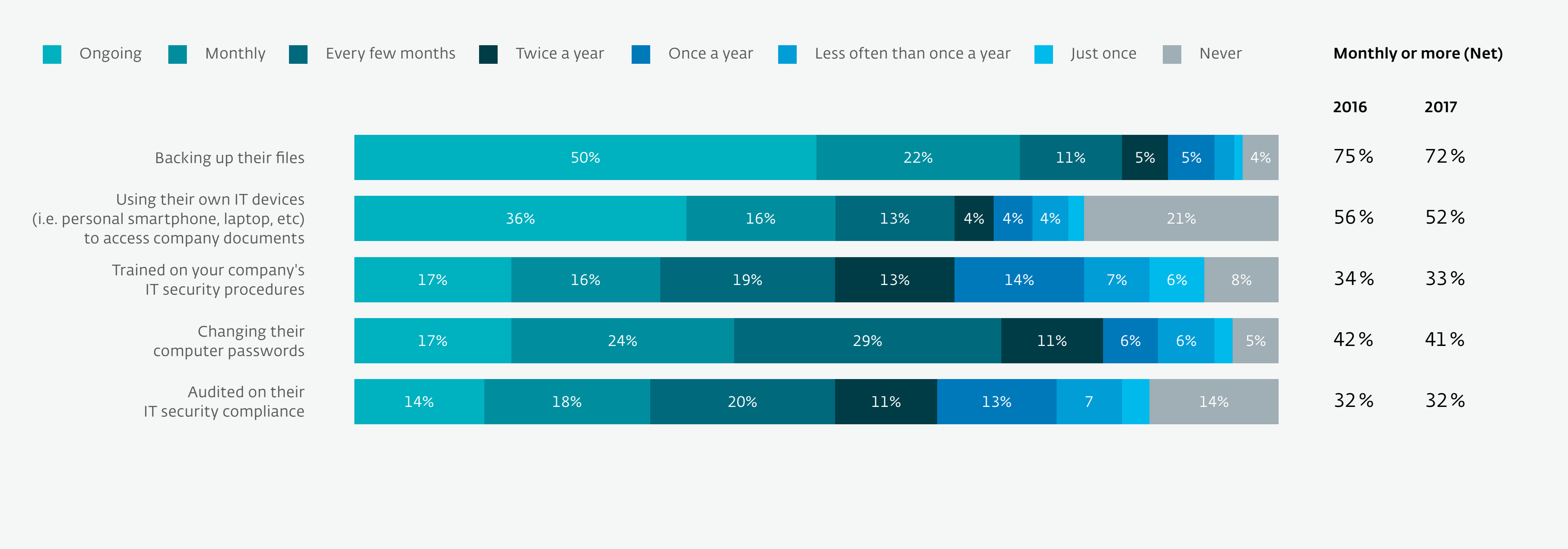


Base: All respondents 2016 (n=1003); 2017 (n=1003)

Staff and IT training

Backing up files is believed to be most common practice among staff– seven in ten (72%) say they preform this task monthly, or more. This is down 3 points from 2016. Half (52%) of employees say that on a monthly basis, staff are using their own IT devices to access company documents, down 4 points.

Q.5 How often is your staff…

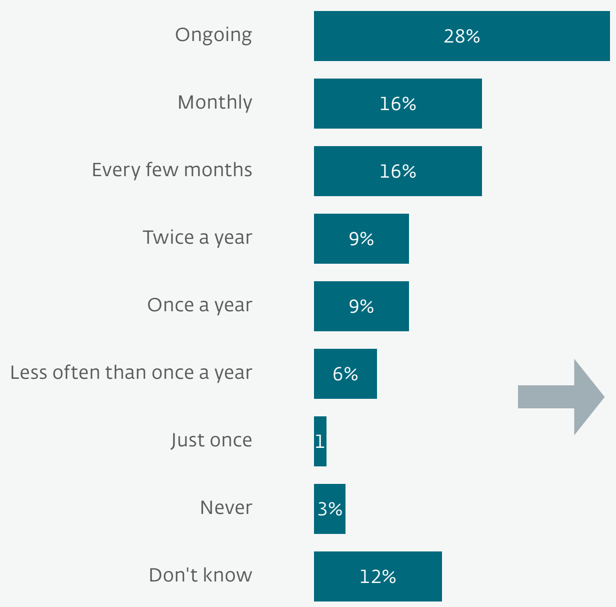


Base: All respondents (n=1003)

How often organizations update cyber security procedures

Less than half (44%) of employees say that their organization updates their cyber security procedures (28% ongoing/16% monthly) on a regular basis. One in four (26%) say it is updated several times a year, one in ten (9%) do so once a year, and 6% say it is updated less often than once a year. Only 3% of employees say it is never updated.

Q.5a How often does your organization update its cyber security procedures?



Medium Businesses (30%) are significantly more likely to say their organization updates its cyber security procedures several times a year, compared to small businesses (21%)

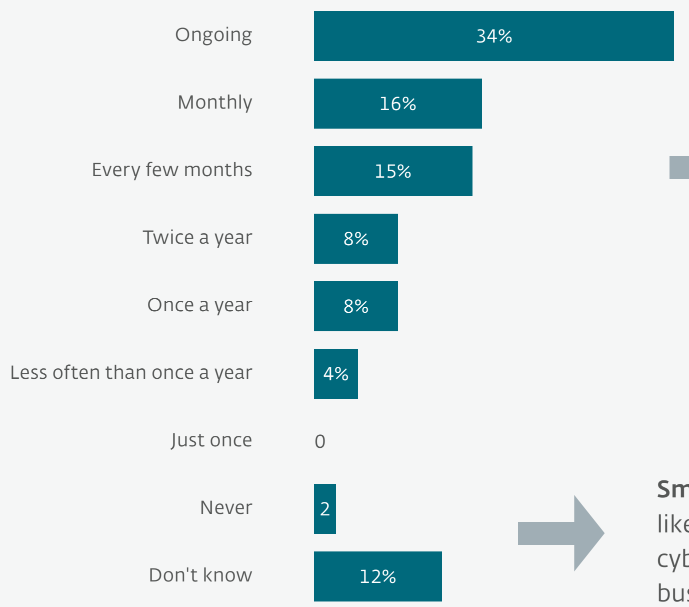
Small Businesses (8%) are significantly more likely to say their organization updates its cyber security procedures less often, compared to medium businesses (5%)

Base: All respondents (n=1003)

How often organizations update cyber security software

Half (50%) of employees say that their organization updates its cyber security software monthly or on a more-frequent basis – including one in three (34%) who say updating software is an ongoing process. Just 2% say that their organization never makes updates, while one in ten (12%) say they don’t know what their company's procedures include.

Q.5b How often does your organization update its cyber security software?



Medium Businesses (26%) are significantly more likely to say their organization updates its cyber security software several times a year, compared to small businesses (20%)

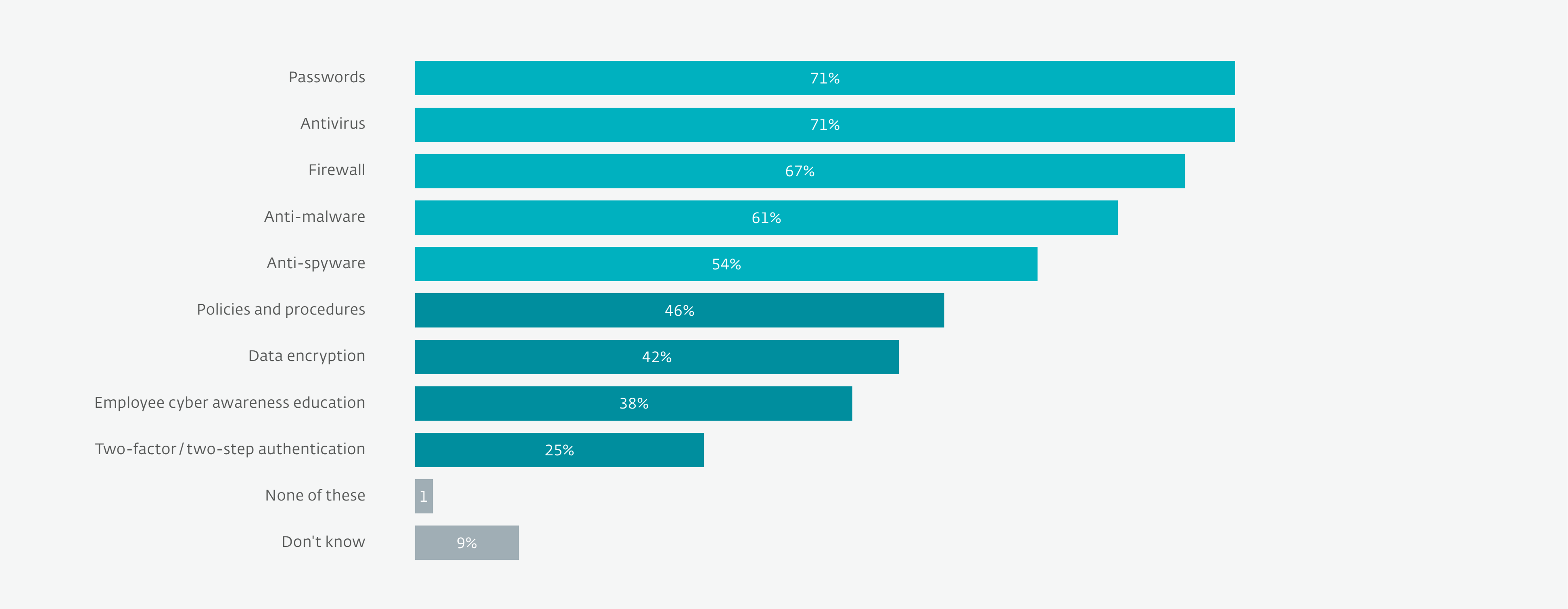
Small Businesses (3%) are significantly more likely to say their organization never updates its cyber security software, compared to medium businesses (1%)

Base: All respondents (n=1003)

Current layers of cyber security in place protecting the business

Almost all (90%) of employees say that their companies have some layer of cyber security protecting their business. The most common forms of cyber security implemented are passwords (71%), Antivirus (71%), Firewall (67%), Anti-malware (61%), and Anti-spyware (54%). Less than one in ten (9%) are unaware of the layers put into place to protect their company, and only 1% say there is nothing in place.

Q.7a Which of the following layers of cyber security do you currently have protecting your business?

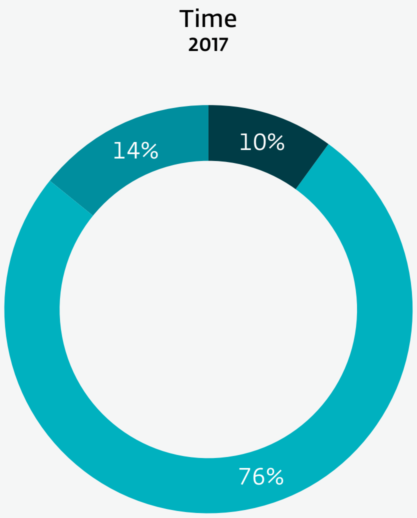


Base: All respondents (n=1003)

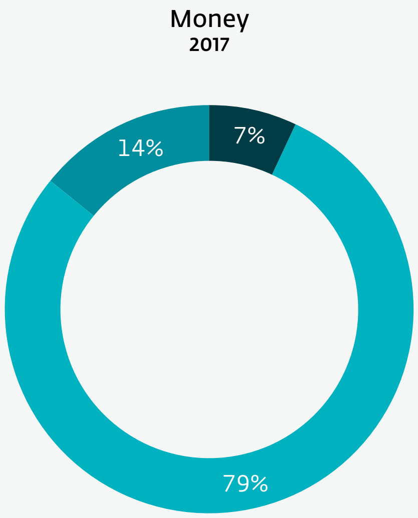
Amount of time and money spent on IT security

Just one in ten employees believe that their organization spends too much time (10%), and money (7%) on IT security — both remaining consistent with 2016. Less than two in ten (14%) employees say their organization does not spend enough time (down 8 points), and money (down 9 points). Overall employees are satisfied with the quantity of resources being devoted to IT security — a majority say that their organization spends the right amount of both time (76%) and money (79%).

Q.8 Do you believe that the amount of time and money that your organization spends on IT security is:



2016	
Too much	8%
About right	70%
Not enough	23%



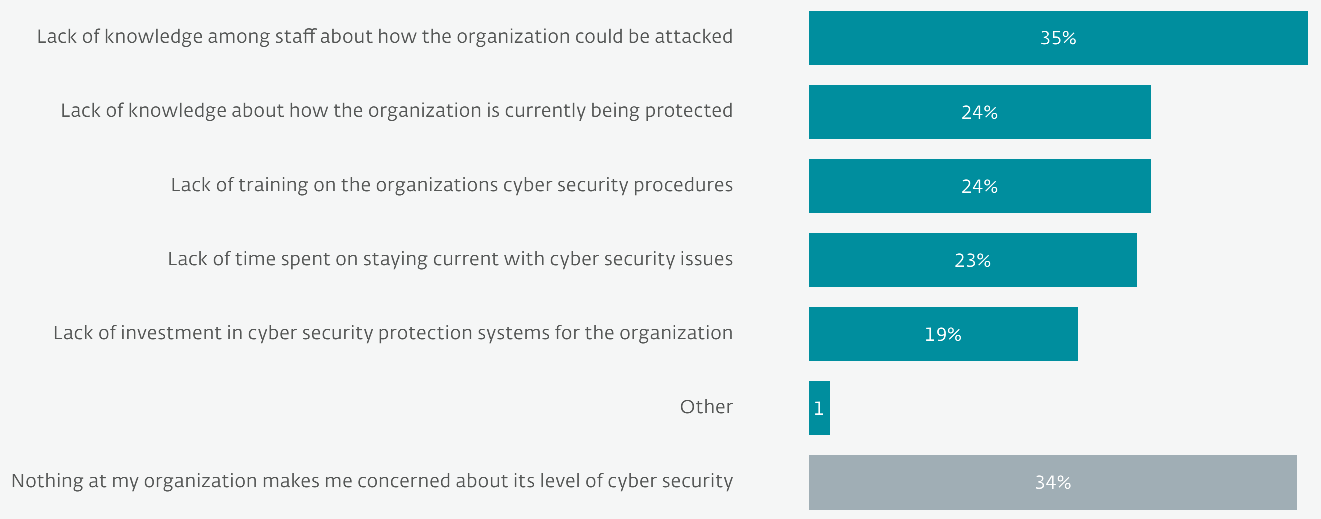
2016	
Too much	8%
About right	70%
Not enough	23%

Base: All respondents (n=1003)

Concerns about level of cyber security

Two in three (66%) employees express some level of concern when it comes to their organization's level of cyber security, whether it be driven by the lack of knowledge, training, and time invested in cyber security procedures. Whereas, only one in three (34%) say that there is nothing at their organization that makes them concerned about its level of cyber security readiness.

Q.8a Which of the following, if any, make you concerned about your organizations level of cyber security?

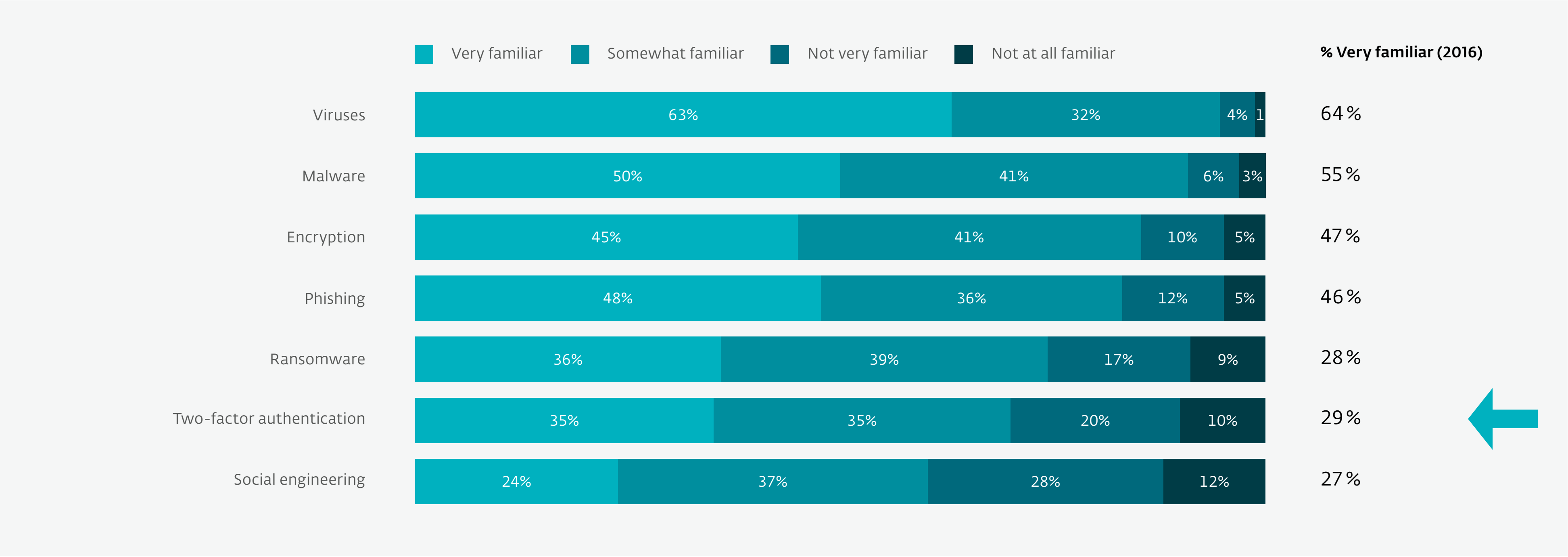


Base: All respondents (n=1003)

Familiarity with IT terms

While familiarity with some terms has risen over the past year, apart from viruses and malware, a minority of employees are still unable to say they are "very familiar" with the remaining IT concepts listed.

Q.9 How familiar are you with the following terms:



Base: All respondents 2017 (n=1003); 2017 (n=1003)

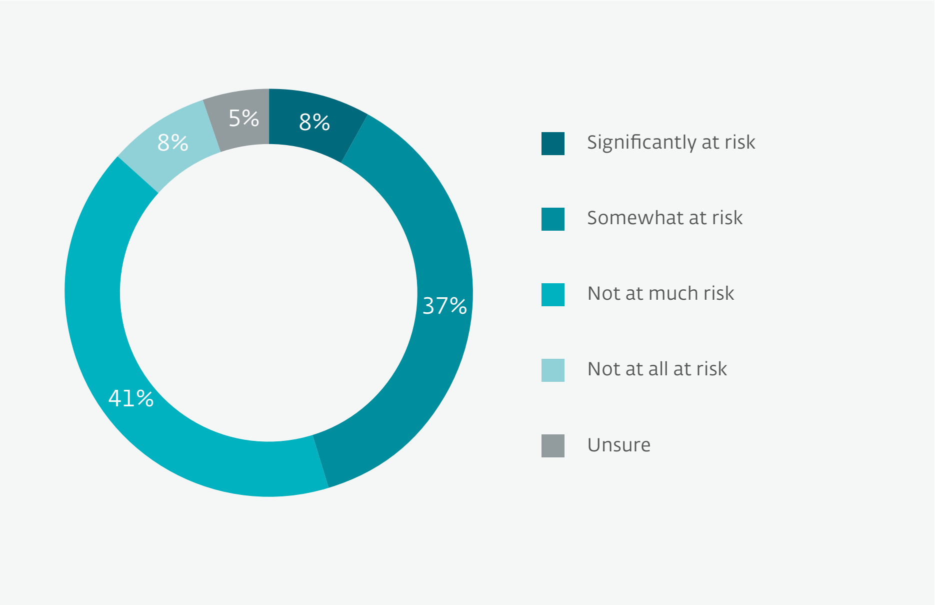
Confidence your business is safe from cyber-attacks

Nearly half (46%) of employees believe that their business is at risk of a cyber security attack, 8% of whom say they perceive their organization to be significantly at risk. If an attack were to occur, only one in four (26%) employees are very confident that their business and its information would be safe, this marks a 7-point drop from 2016.

46%

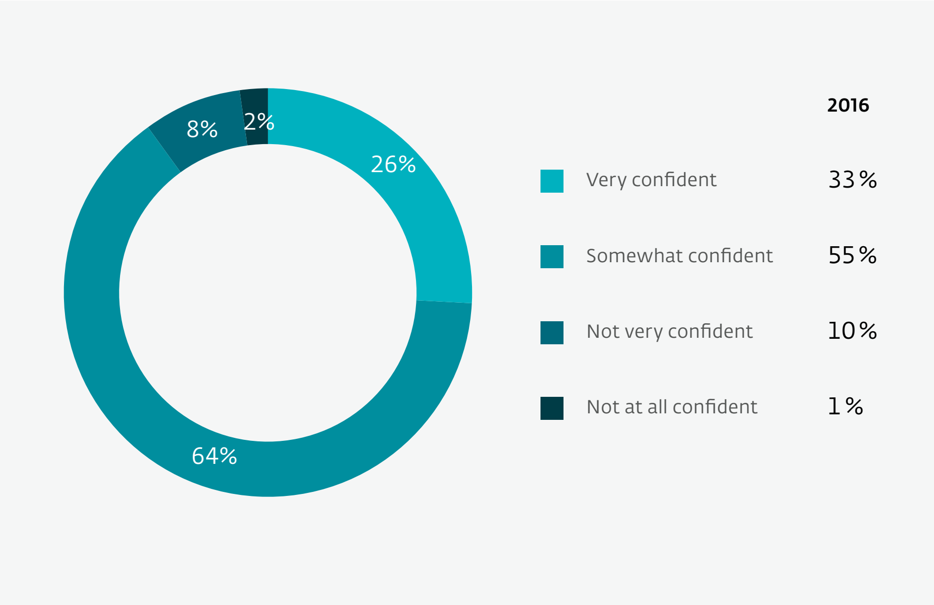
of employees believe that their business is at risk of a cyber-security attack

Q.9a To what extent do you think your business is at risk of a cyber security attack?



Base: All respondents 2016 (n=1003); 2017 (n=1003)

Q.10 How confident are you that your business and its information is safe from cyber-attacks?

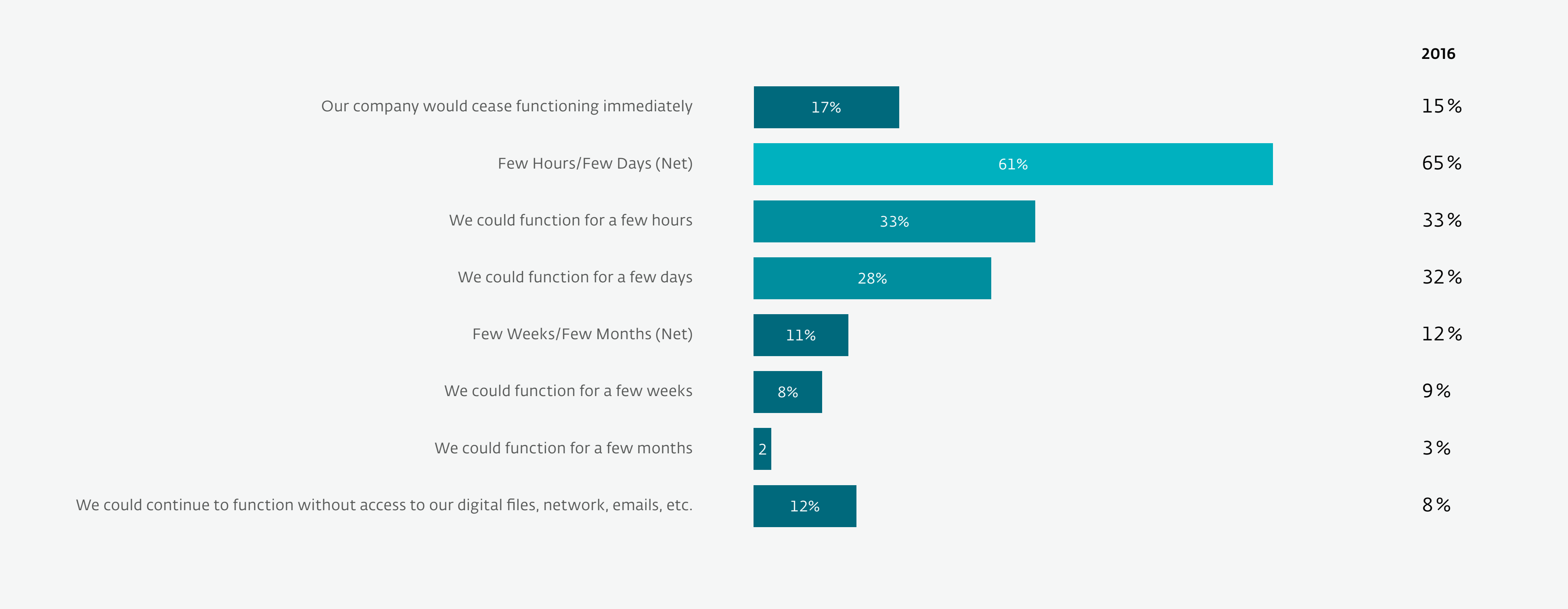


Base: All respondents 2016 (n=1003); 2017 (n=1003)

Time your business can function without digital files

Nearly two in ten (17%) employees believe if their business were to experience an attacked, the company would cease functioning immediately, being unable to have access to its digital files, the network, emails, etc. Conversely, six in ten (61%) believe they could function without digital access for few hours/few days, and one in ten (11%) say they would be fine for a few weeks/few months.

Q.12 How long do you think your business could function without access to its digital files, the network, emails, etc?



All respondents 2016 (n=1003); 2017 (n=1003)

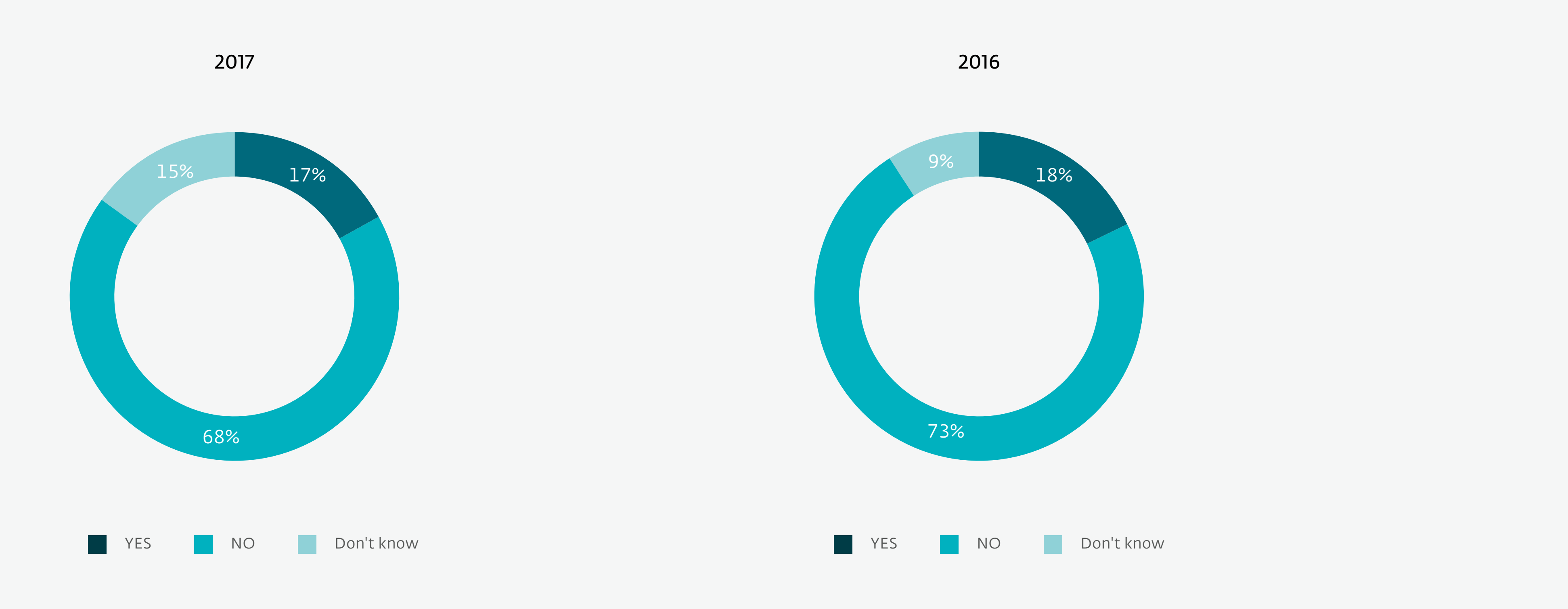
Victim of a cyber-attack

Remaining consistent with 2016, nearly two in ten (17%) employees say that their organization has been the victim of a cyber-attack.

17%

employees say that their organization has been the victim of a cyber-attack

Q.14 Has your organization ever been a victim of a cyber-attack?

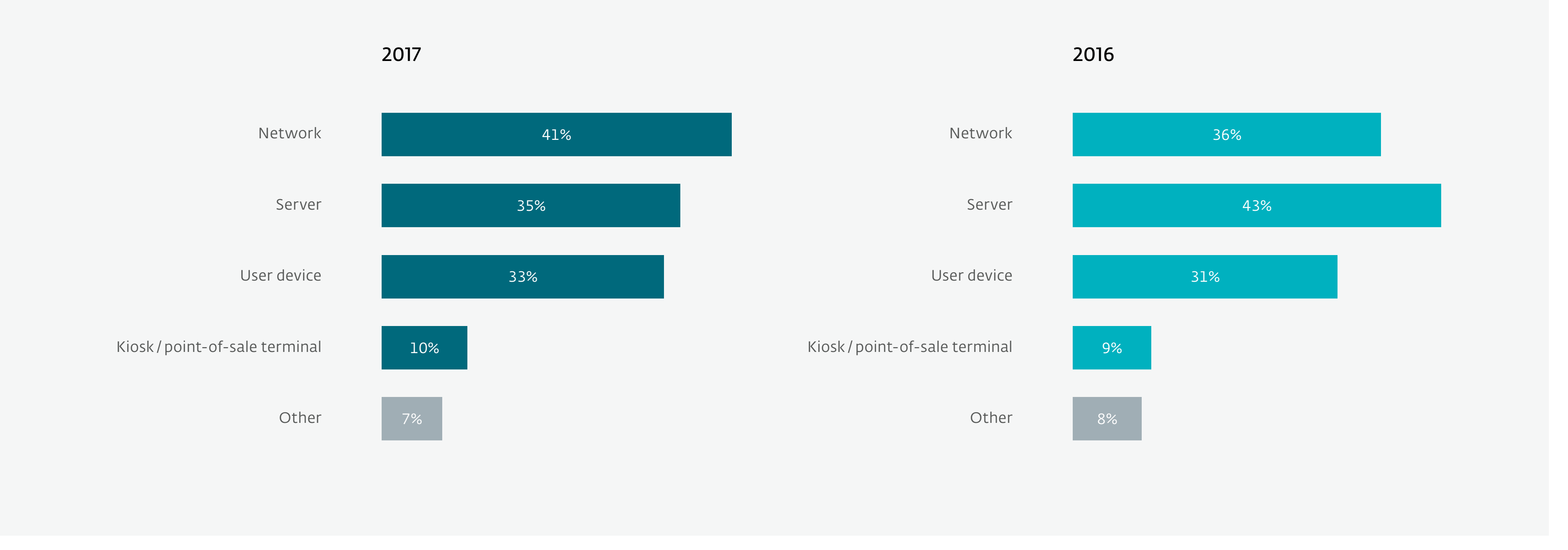


Base: All respondents 2016 (n=1003); 2017 (n=1003)

What was hacked

Among the two in ten (17%) employees whose company has been a victim of a cyber-attack, the most common areas hacked were the network (41%, +5 pts), and the server (35%, -8 pts). Other areas that were targeted were the user device (33%) and kiosk/point-of-sale (10%).

Q.15 What was hacked?

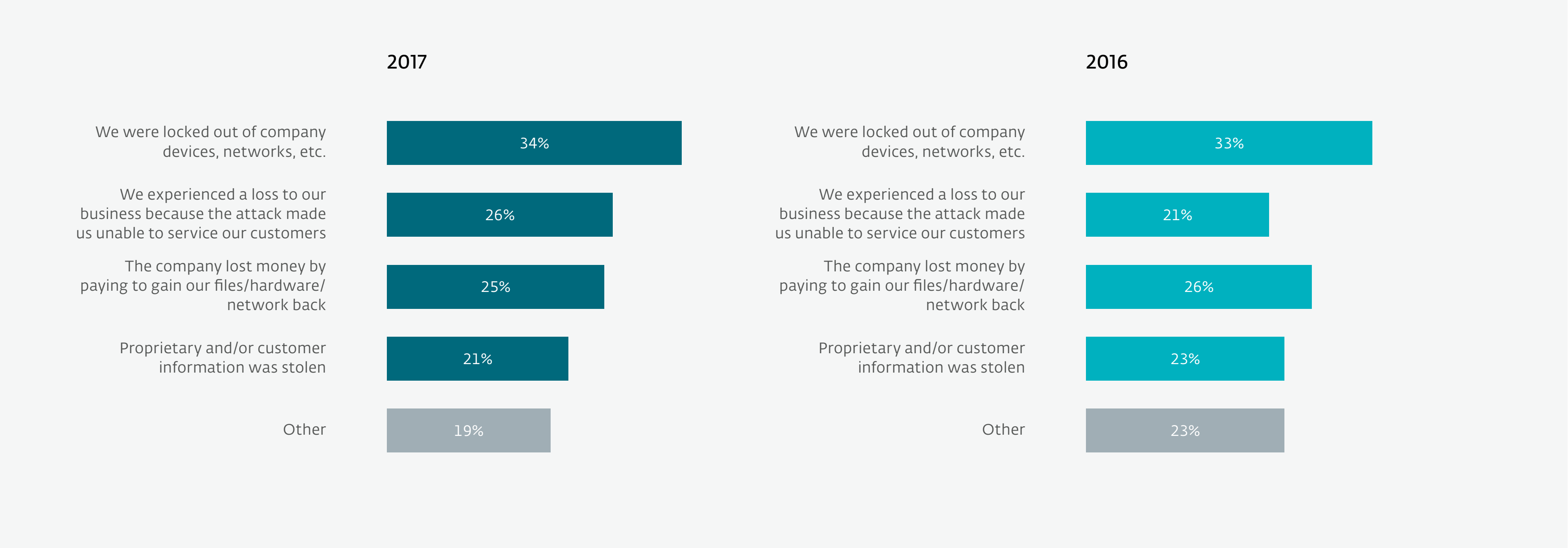


Analyzed Respondents: Victims Of Cyber-Attack 2016 (n=175); 2017 (n=173)

Nature of the attack

During the attack, more than one third (34%) of employees say they were locked out of company devices. Cyber-attacks reported this wave were likelier to experience a loss to their business because the attack made them unable to service their customers (26% vs. 22% in 2016). A further one in four (24%) lost money by paying to gain back their files, and 21% had propriety and/or customer information stolen.

Q.16 Which of the following best describes the nature of the attack?



Analyzed Respondents: Victims Of Cyber-Attack 2016 (n=175); 2017 (n=173)

Part 3: Tips to set your business up for success

Cybersecurity provides a stable foundation and allows you to stay competitive. Here are five proactive tips to implement today.

1. Assess your risk

How you run your business and the kind of data you hold impacts the level of risk to your business. Organizations of all sizes generate and store data that could be of interest to cyber criminals. Consider how valuable or sensitive each set of data is, by performing a security audit, to determine the unique mix of software, solutions, and IT policies and procedures needed to achieve appropriate protection.

2. Educate your staff

Employees are a business' first line of defense, so training them in cybersecurity best practices and developing a proactive security plan is integral to building confidence with your customers. ESET experts have developed a free cybersecurity awareness training program, which is available for download and distribution by any organization to its employees, regardless of whether they use ESET's software or not. The program takes less than 90 minutes to complete and provides progress tracking and certification. Visit *eset.ca/cybertraining* to get started.

3. Deploy a multi-layer, multi-vendor security solution

The best strategy is to make an attackers' job as difficult as possible by having security at every level to prevent breaches. For reliable and strong cybersecurity defenses, companies should opt for a solution that offers multiple complementary technologies, with high detection rates and a low number of false positives. That way, if one technology layer is bypassed, an array of others are in place to take action and keep information protected.

4. How updates make your security solution stronger

Anti-malware software installed on endpoints such as computers and mobile devices must be kept up to date to be equipped to recognize and defend against the latest threats. A great feature of ESET products is that software updates are made automatically, keeping devices always current with the most recent protection available. In addition to lower false positive rates, the updated solution can use data to create a reliable threat database stored in the cloud. By sharing with all recognized devices, this can protect users from a wider array of malicious items.

5. Outsource IT support

One way to ensure attention is focused on the growth and development of your company, is to consider outsourcing IT. IT partners and trusted tools can provide proactive, preventative support that allow you to scale and upgrade security services to fit your business' growing needs. Doing so will free up space and time to invest in your business and employees.

Part 4: Methodology

- These are findings of an Ipsos poll conducted on behalf of ESET.
- For this survey, a sample of 1,003 Canadian employees 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 were interviewed from the Ipsos I-Say panel. The study was fielded from August 28th to September 7th, 2017.
- Quotas and weighting were employed to ensure that the sample's composition reflects the overall population according to census information.
- The precision of online polls is measured using a credibility interval. In this case, the results are accurate to within +/-3.5 percentage points, 19 time out of 20, of what the results would have been had all Canadian employees of small and medium businesses in these job functions been polled.
- Credibility intervals are wider among subsets of the population.

1003

Canadian SMB employees who work in IT were interviewed for this survey

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 ranks third in the global research industry. With a strong presence in 87 countries, Ipsos employs more than 16,000 people and has the ability to conduct research programs in more than 100 countries. Founded in France in 1975, Ipsos is controlled and managed by research professionals. They have built a solid Group around a multi-specialist positioning — Media and advertising research; Marketing research; Client and employee relationship management; Opinion & social research; Mobile, Online, Offline data collection and delivery.

Ipsos is listed on Eurolist — NYSE — Euronext. The company is part of the SBF 120 and the Mid-60 index and is eligible for the Deferred Settlement Service (SRD). ISIN code FR0000073298, Reuters ISOS.PA, Bloomberg IPS:FP

To learn more, visit *www.ipsos.com*.

ESET Canada

For 30 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.

Evolving threats require an evolving IT security company. Backed by R&D centers worldwide, ESET becomes the first IT security company to earn 100 Virus Bulletin VB100 awards, identifying every single “in-the-wild” malware without interruption since 2003. For more information visit *www.eset.com* or follow us on LinkedIn, Facebook and Twitter.

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

ESET business products can be sourced through a vast reseller partner network across Canada and North America. Consumer products are available at Best Buy and Staples, and online at *www.eset.com*.

To begin setting your business up for success or to simply provide feedback, contact the ESET Canada office at 1-844-423-3738 or *feedback@eset.ca*.