From putting faith in others to taking responsibility

Three key cybersecurity trends in the business community

Your world. Our domain.

Contents

1 Introduction

In April 2020, market research agency GfK carried out a survey of SMEs for SIDN. Roughly fifty questions were answered by 577 respondents from businesses with more than ten full-time employees. The survey examined a range of cybersecurity issues. Are businesses aware of the cybersecurity risks they face, and what are they doing about them? Are proprietors worried about their businesses?

This report considers the main findings of the survey, including the observation that more respondents reported being affected by cybercrime than when we last investigated trends in online security and e-identity in 2018. The role of the IT service provider is also examined: do SMEs perhaps overestimate the protection that their IT partners can provide?

A strange disconnect seems to be developing. Although the number of firms falling victim to cybercrime is on the up, people in the SME sector aren't very worried about the threat of cybercrime or its consequences. How serious are you about keeping your business safe? Do you have a clear picture of where your firm is vulnerable, or do you simply trust someone else to take care of things? Think seriously about cyber-resilience and take steps to protect yourself!

2 Management summary

Market research agency GfK recently carried out a survey of security awareness in small and medium-sized enterprises (SMEs) for SIDN. This report describes the survey's main conclusions.

Conclusion #1: The proportion of SMEs falling victim to cybercrime has risen from 19 to 22 per cent.
There is a persistent misconception that cybercrime mainly affects corporates. In reality, SMEs are easier and more attractive targets. The reason being that SMEs often lack the resources, knowledge and/or access to knowledge required to recognise threats and protect against them. Against that background, the proportion of SMEs falling victim has gone up by three percentage points since our last survey.

Ransomware heads the list of perceived cybercrime threats by a wide margin. And the evidence is that paying a ransom doesn't always resolve the matter for firms that get hit. What's more, criminals often gain access not by exploiting technical weaknesses, but by exploiting staff (who usually have no idea that they're being used). The main way of doing that is by sending e-mail (phishing).

Conclusion #2: The business community is increasingly worried about cybercrime.
The business community is becoming more worried about cybercrime. The proportion of SMEs that rate cybercrime as at least a moderate threat is up slightly since our last survey, to 22 per cent. The steps most widely taken to counter the threat are using antivirus software, using a strong e-mail spam filter and regularly updating or replacing equipment.

When it comes to making cybersecurity arrangements, the biggest problem businesses have is that developments move so quickly that it's hard to keep up. Some also find the cost of security problematic.

Conclusion #3: Most SMEs are happy to leave cybersecurity to their IT service providers.
SMEs have a lot of faith in their IT service providers; 79 per cent of surveyed SMEs were confident that their IT partners had cybersecurity under control. Yet 58 per cent of those service providers reported that their SME customers weren't properly protected…

It's common for SMEs to assume that IT service operators have a duty of care and are providing at least some level of cyber-protection. However, formal arrangements are made in only 22 per cent of cases. What's more, IT people aren't necessarily cybercrime experts: security is a separate field from performance and availability.

3 Conclusion #1: The proportion of SMEs falling victim to cybercrime has risen from 19 to 22 per cent

There is a persistent misconception that cybercrime mainly affects corporates. In reality, SMEs are easier and more attractive targets. The reason being that SMEs often lack the resources, knowledge and/or access to knowledge required to recognise threats and protect against them. Against that background, the proportion of SMEs falling victim has gone up by three percentage points since our last survey. The five forms of cybercrime most widely perceived as threatening by survey respondents were malware, phishing, ransomware, data leakage and data theft.

Of those five cybercrime threats, ransomware heads the list by a wide margin. That finding backs up the conclusion of a Help Net Security study into ransomware.

Help Net Security surveyed more than five hundred managers working in the SME sector and found that 78 per cent of firms active in the B2B market had paid a ransom at one time or another. Amongst those focusing on the B2C market, the figure was 63 per cent.

What is ransomware?

Ransomware is a particular type of malware (malicious software) designed to prevent legitimate users accessing computers or data. As the name suggests, a ransom is demanded for releasing the equipment or files, typically payable in the digital currency Bitcoin. Ransomware is sometimes referred to as 'cryptoware.

EDo victims who pay the ransom get their data back?

Ransomware victims who pay up don't always get their files back undamaged. That's confirmed by security firm Proofpoint's State of the Phish survey. Proofpoint got feedback from more than six hundred IT security professionals in various countries, including the USA, the UK and Germany. And they found that, while 69 per cent of victims who paid up regained access to their systems, 22 per cent got nothing for their money. Their data either remained blocked or was irreparably corrupted.

What weaknesses do scammers exploit?

The research into trends in online security and e-identity that GfK did for us in 2018 found that a lot more could be done to prevent staff being exploited by cybercriminals. No less than 32 per cent of incidents reported to SecureMe2 (an organisation offering high-grade protection against cybercrime to SMEs) began with some form of human action. In other words, there's a one-in-three chance of one of your own people being the weakness that scammers use to attack your business. The main strategy used is phishing: sending trick e-mails with ransomware or malware links. And, unfortunately, attacks like that can't be prevented by anti-virus software.

3 Conclusion #1

However, it's good news that employees often form the weak link when it comes to protecting against cybercrime. Because employees can be educated to minimise the threat. Everyone within an organisation should be able to answer questions such as "What forms of cybercrime are there?", "How do I recognise them?" and "What should I do about them?" If you'd like to know more about how to educate your staff, read our whitepaper Making SMEs cyber-resilient.

In the following section, we consider whether SMEs are actually worried about cybercrime. Many say that they aren't, but it does seem that things are changing. We also explore what SMEs are doing to protect themselves.

> Chart 1: Has your business been affected by cybercrime in the last twelve months?

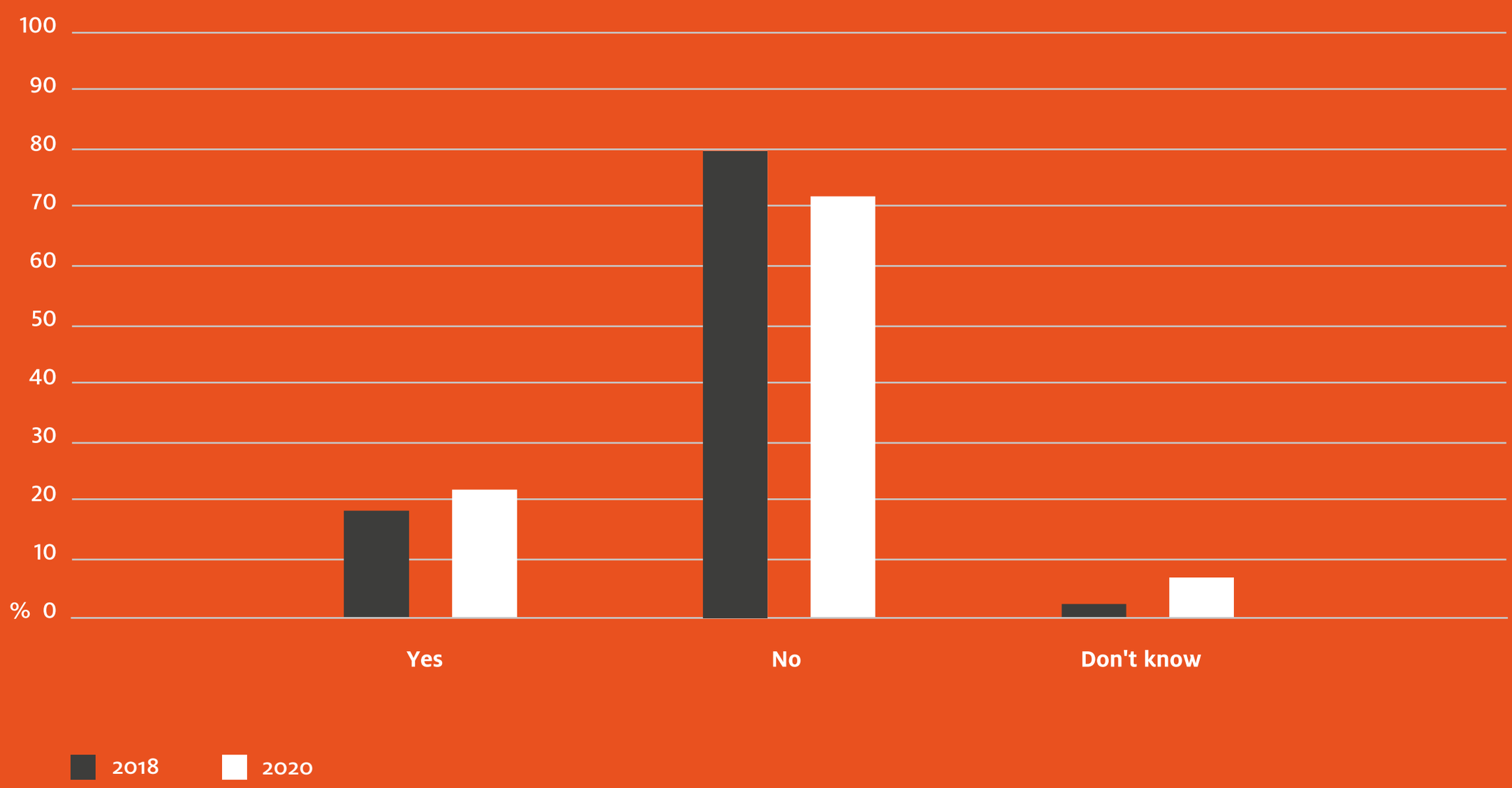


Chart 1: Has your business been affected by cybercrime in the last twelve months? (source: GfK n=512 (2018) n=577 (2020))

4 Conclusion #2: The business community is increasingly worried about cybercrime

In GfK's recent survey for us, respondents were asked, "How big a threat do you think cybercrime is to your business?"

And it seems that the business community is becoming more worried about cybercrime. The proportion of SMEs that rate cybercrime as at least a moderate threat is up slightly at 22 per cent, while 57 per cent now say it is at least a minor threat. In GfK's 2019 survey, 9.9 per cent of respondents described cybercrime as a moderate threat. There has therefore been a significant rise in threat perception in a relatively short space of time.

In the latest survey, one in ten SMEs that labelled cybercrime a moderate threat said that the continuity of the business could even be at stake.

What security measures do businesses take?

1. 62 per cent have good anti-virus software
2. 52 per cent use a strong e-mail spam filter
3. 47 per cent regularly replace or update equipment
4. 43 per cent have extra Wi-Fi network security
5. 40 per cent have strict password policies
6. 40 per cent use cloud-based external data storage

Where do SMEs run into difficulties?

When it comes to making cybersecurity arrangements, the biggest problem businesses have is that developments move so quickly that it's hard to keep up. Some also find the cost of security problematic. Another common complaint is that many security solutions aren't well tailored for smaller businesses, particularly in terms of price.
In the following section, we share our findings on SMEs' confidence in their IT service providers when it comes to cybersecurity. Are SMEs perhaps too confident?

> Chart 2: What cybersecurity measures has your business taken?

"Many businesses believe that having a virus scanner and firewall is enough to provide protection. Unfortunately, that isn't the case any longer. A virus scanner can only flag up known threats. It doesn't look out for abnormal network traffic, for example, and it can't detect novel intrusions. A firewall is similarly incapable of keeping out all hazardous network traffic."

Liesbeth Kempen, IT Security Management Consultant

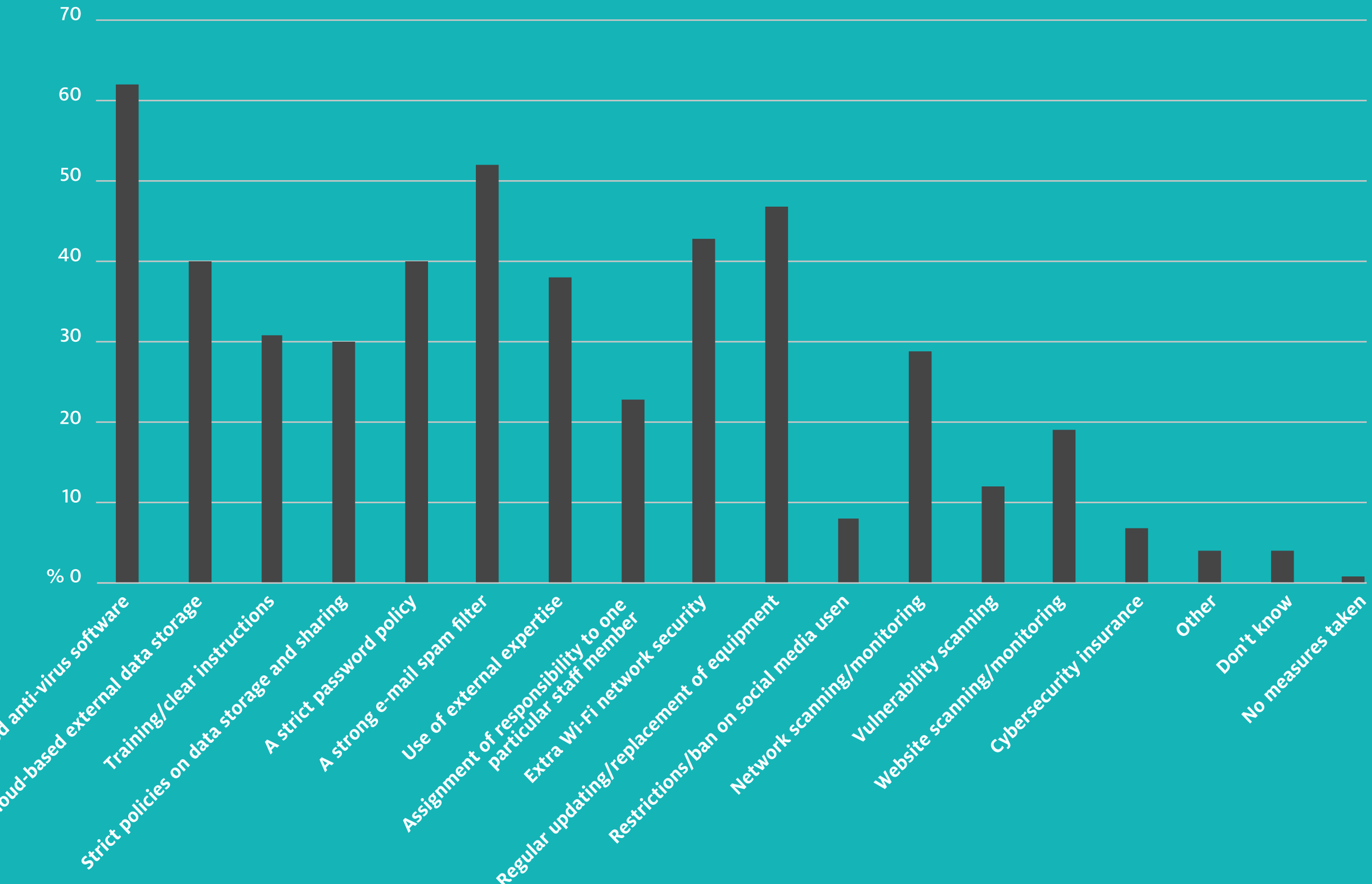


Chart 2: What cybersecurity measures has your business taken? (source: GfK, n=577)

5 Conclusie #3: Most SMEs are happy to leave cybersecurity to their IT service providers

GfK's survey found that SMEs have great faith in their IT service providers where cybersecurity is concerned. No fewer than 79 per cent agreed with the statement, "I'm confident that our IT service provider has cybersecurity under control." Their confidence is based mainly on communication about security measures, the speed at which incidents are reported, and reputation. However, research by insurer Centraal Beheer revealed that IT service providers believe that 58 per cent of their SME customers don't have adequate security.

Do SMEs perhaps overestimate the protection that their IT partners can provide?
It's common for SMEs to assume that IT service operators have a duty of care and are providing at least some level of cyber-protection. However, formal arrangements are made in only 22 per cent of cases. What's more, IT people aren't necessarily cybercrime experts: security is a separate field from performance and availability.

Security service providers differ from IT professionals mainly in terms of how quickly and how often they provide customers with information about security matters. For example, the IT professionals may well have no role in the purchase of a company's internet-enabled devices. Besides which, cybersecurity isn't an exclusively technical issue. How do staff deal with suspect links and phishing mail? Good practice is just as important as good anti-virus software. And it takes time to develop good practices, with relatively few IT service providers providing appropriate support.

How serious are you about keeping your business safe?
Our findings may well have given you a few pointers as to how worried you should be about your business's cybersecurity. Or perhaps 'horror stories' involving your peers have convinced you that it's time to protect yourself against cybercrime.

Sadly, there is no such thing as total security. There is, however, a lot you can do to reinforce the protection provided by a virus scanner and firewall. Crucially, you need a clear picture of the online security risks facing your business. Because every business, no matter how small, has something worth taking. And nowadays every business is a potential target for hackers equipped with automated tools, which they turn on one website after another.

If you're serious about protecting the continuity of your business, you can't afford to neglect your cyber-resilience. After all, if something does go wrong, ultimate responsibility and liability lie with you.

> Chart 3: To what extent do you agree with the following statement – "I'm confident that our IT service provider has cybersecurity under control."

> Chart 4: You expressed confidence in your IT service provider(s). What is your confidence based on?

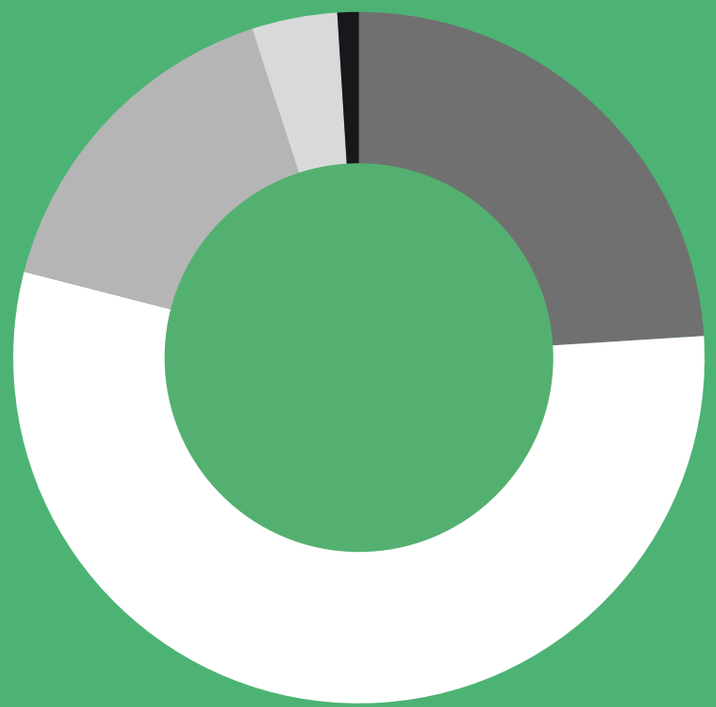
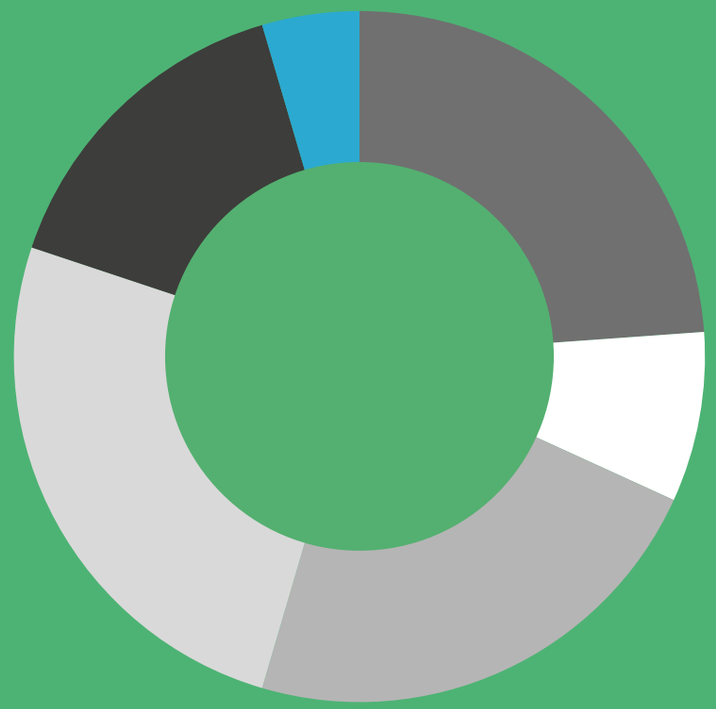


Chart 3: To what extent do you agree with the following statement – “I’m confident that our IT service provider has cybersecurity under control.” (source: GfK, n=577)



They keep us informed about their cybersecurity measures

They provide a dashboard for continuous status monitoring

They have a market reputation for expertise

They inform us promptly about incidents

They have a track record with us

Other

Chart 4: You expressed confidence in your IT service provider(s). What is your confidence based on? (source: GfK n=458)

6 How serious are you about keeping your business safe?

Any SME looking to keep cyber-threats at bay ideally wants malicious traffic to be detected as soon as it enters the company network. Entry-point traffic can then be analysed on the basis of behaviour, destination and timing. And anything unusual can be picked up early, enabling speedy intervention. Unfortunately, however, detection reports are hard to interpret, especially for non-specialists. That's why we've developed CyberSterk. CyberSterk gives you a clear picture of the online security risks facing your business. Your network and website are carefully monitored -- by the CyberSterk Box, for example. That's a small security device that we connect to your system.

We also analyse your network traffic in real time. As soon as anything undesirable or suspicious is detected, we sound the alarm. And all risks are reported in clear language on a personalised dashboard. Enabling you to act quickly and keep your business running smoothly and safely. With a clear picture of what's wrong, you're able to have a proper discussion with your IT partner about how to resolve detected weaknesses in your set-up. And, if you don't have an IT partner, our CyberSterk support team can provide the advice and solutions you need.

SIDN CyberSterk

Want to learn more about what CyberSterk can mean for your business?
https://www.cybersterk.nl/
https://www.sidn.nl/en/product/cybersterk

What our service involves

- We make a weekly remote scan of your website to pick up any site-related risks.
- We connect a CyberSterk Box to your company network. The Box detects any abnormal internet traffic on your network, as well as attacks from outside. If anything suspicious shows up, we sound the alarm.
- We report your scan results in clear language on a user-friendly personal dashboard. It's fully mobile-compatible, so you can get issue notifications on your phone.
- We run periodic phishing simulations and measure how your staff respond.
- Once a month, we'll also send you a report setting out the main scan results.
- If you're stuck with anything, you can contact your IT partner or our support team, and we'll find a solution together.

We are SIDN

We are SIDN: the Foundation for Internet Domain Registration in the Netherlands. We've been responsible for running the .nl domain since 1996. Our mission is connecting people and organisations to promote problem-free, opportunity-rich digital living. We contribute to the security of the Dutch internet, conduct cybersecurity research and monitor for suspect behaviour. The development of new services, such as CyberSterk, is a key feature of that activity portfolio.

Colophon

This report presents the highlights of a survey carried out for SIDN by GfK.
Contributors:

GfK
Henk Delfos – Industry Lead
Erica Nagelhout – Senior Research Manager Consumer Insights

SIDN
Christiene Bouwens – Marketing Manager
Michiel Henneke – Marketing Manager
Martin Sluijter – Communications Advisor

Canvass Company
Esther Derks – Business Journalist

If you've got any questions about the survey, please mail
communicatie@sidn.nl

Subscribe to our newsletter
www.sidn.nl/nieuwsbrief

SIDN
PO Box 5022
6802 EA Arnhem, The Netherlands
Meander 501
6825 MD Arnhem, The Netherlands
T +31 (0)26 352 55 00
www.sidn.nl