From awareness to action:
Trends in Online Security & e-Identity

Connectis

SIDN Your world. Our domain.

Contents

1 Introduction & structure

In the Netherlands, using the internet is generally problem free: it's easy to get on line, and the .nl domain is one of the most secure in the world. The second of those factors is partly due to the combined efforts of SIDN and Connectis. We manage the national domain with professional care, we constantly look to innovate, and we develop online authentication solutions to enable safe log-ins. We also carry out research to support our goals, such as the survey of trends in digital security and e-identity reported here.

Central to this research is the concept of trust. Do enterprises and consumers have confidence in the security of the internet? Are they aware of the risks, and what are they doing about them? Are they worried about their online privacy? Since 2012, we've been seeking answers to such questions through our surveys of general trends in internet use.

And those surveys have highlighted security and identity as increasingly prominent themes in the general picture. This year, SIDN and Connectis therefore decided to investigate trends in online security and e-identity more closely. First, a survey was carried out to gauge the feelings of consumers and businesspeople. The findings were then assessed with the help of an expert panel. With our two-part research method, we hoped to illuminate the current online security and e-identity landscape, and gauge the future impact of trends such as the rise of the Internet of Things.

Survey method

The survey involved gathering online feedback from a representative group of 2,095 Dutch consumers and 512 businesses of various sizes. All survey participants were members of GfK's Online Research Panel (CAWI). The survey took place in February and March 2019.

Expert panel

The survey findings are presented in this report, together with analysis by a panel of carefully selected experts. The panel debated five topics to explore the issues that currently dominate the field of cybersecurity and e-identity: where are organisations most vulnerable, what implications does the Internet of Things (IoT) have for online security, and who is responsible for protecting us: the market? The government? Or should we protect ourselves?

> About the expert panel

We are SIDN
SIDN (the Foundation for Internet Domain Registration in the Netherlands) has been responsible for running the .nl domain since 1996.
Our mission is connecting people and organisations to promote safe and convenient digital living. In partnership with around 1,200 ‘registrars’, we ensure that all 5.8 million-plus .nl domain names remain reachable.
SIDN additionally processes registrations and register amendments, handles disputes and contributes to the security of the internet in the Netherlands.
Other activities include cybersecurity research and monitoring to detect suspect behaviour. In connection with those activities, we also develop new services, such as the Domain Name Surveillance Service (DBS).

We are Connectis
Connectis connects organisations, consumers and countries with solutions for online identification and authentication. We provide a platform that enables users to log in to on-line services using DigiD, eHerkenning, iDIN, eIDAS, social logins and numerous other systems. More than 350 organisations now use the Connectis Identity Broker to authenticate fourteen million users. And our software and eHerkenning tokens are used by upward of fifty thousand organisations to log in securely to public and private services. Connectis was founded in 2008 and has been part of SIDN since 2017.

2 Cybercrime: businesses underestimate the risks

Cybercrime isn't a problem for businesses that don't have webshops and don't provide online services. Hackers mainly go after banks and other organisations that handle a lot of money. Right? Our expert panel made the point that such popular myths continue to cause a lot of problems. The panel therefore began by discussing the issue of awareness: are businesses sufficiently aware of the risks posed by cybercrime?

Respondents don't appreciate the danger

Many businesspeople still believe that hackers won't be interested in them if they aren't in the ICT industry and don't sell on line. Only 9.9 per cent of the survey respondents who don't provide online services believe that cybercrime is a threat to their organisations. The great majority (90.1 per cent) said that cybercrime wasn't a (serious) threat. Although the split was different amongst online service providers, a broadly similar outlook prevailed, with about 80 per cent saying that cybercrime wasn't a threat. Overall, 67.7 per cent of respondents rated cybercrime a minor threat, while 17.6 per cent said it wasn't a threat at all.

> Chart 1: How big a threat do you think cybercrime is to your organisation? (Source GfK, n=512)

Reality check: every business is an ICT business

Are people right to be so relaxed about cybercrime? The panel was unanimous: greater awareness is needed. Because the reality is that even firms that don't sell goods or services over the internet are interesting to cybercrooks, and they're often easy prey. Everyone has something worth stealing: log-ins, personal data or sensitive business information, for example. What's more, smaller businesses are often targeted as a way of reaching larger suppliers or customers. Because operational and business processes are almost universally digitised, crooks can access them via the internet – sometimes with incredible ease. And, if that happens, the repercussions can be huge. Panellist Maria Genova -- journalist and author of *WHAT THE HACK!* and *Komt een vrouw bij de h@cker* -- is familiar with the scenario:

> *"I know of a transport business where crucial data was held hostage by cybercriminals. The crooks managed to get ransomware onto the company's system, which blocked access to order data and customer details. The organisation was crippled, their trucks were standing idle. The hackers demanded €30,000 to release the data. With digitisation, every business has become an ICT business. People often overlook that."*
>
> *Maria Genova (journalist, writer and speaker)*

Cybersecurity: an IT issue?

Another problem is that many businesses see cybersecurity as a technical issue, according to the panel. It's therefore left to the IT department or even a single technician, who is expected to make sure that everything's secure. However, ICT people aren't necessarily cybercrime experts: security is a separate field from performance and availability. With the rise of the Internet of Things, for example, the ICT department may not be involved with the purchase of all a company's internet-enabled devices. Besides which, cybersecurity isn't an exclusively technical issue. Ensuring that people throughout the organisation do the right thing with suspect links and phishing mail is just as important as having good antivirus software. Perhaps more important.

Investment in cybersecurity is barely increasing

All panellists agreed that much remains to be done in terms of creating awareness and a sense of urgency. But what about cybersecurity expenditure: is it still disappointingly low? Our survey found that cybersecurity budgets remained almost unchanged over the last twelve months. Even amongst respondents who saw cybercrime as a real threat, 69.4 per cent reported that no more money had been made available for securing business processes. In other words, a higher threat perception has little influence on businesses' willingness to invest more.

> Chart 2: What change, if any, do you expect in your organisation's budget for cybercrime prevention over the next twelve months?

"Online security shouldn't be regarded as a self-contained field; it should be integral to the organisation as a whole."

Kees Monshouwer (Monshouwer Internet Diensten)

Cybercrime threat rated highest by online service providers

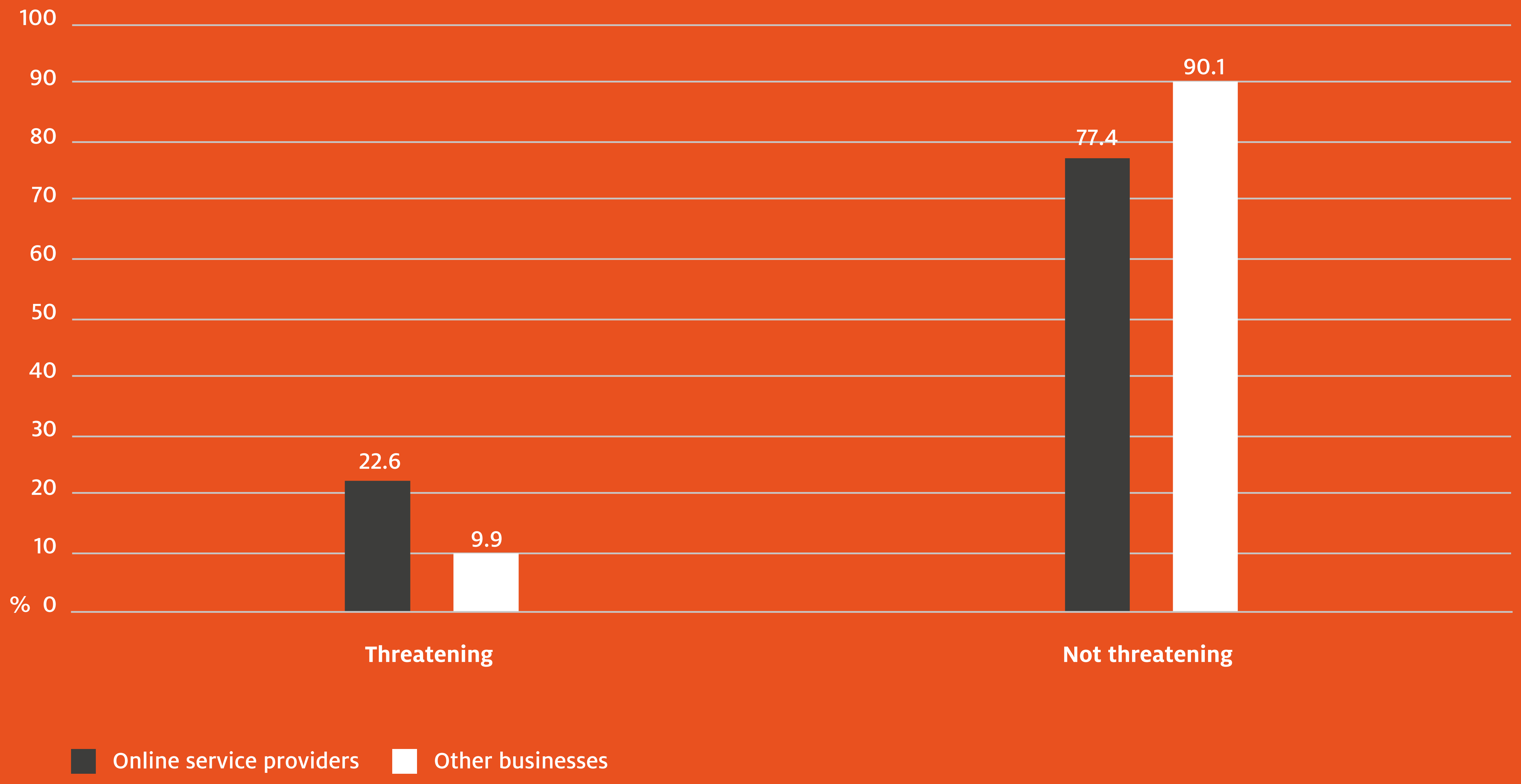


Chart 1: How big a threat do you think cybercrime is to your organisation? (Source GfK, n=512)

Investment in cybersecurity stable

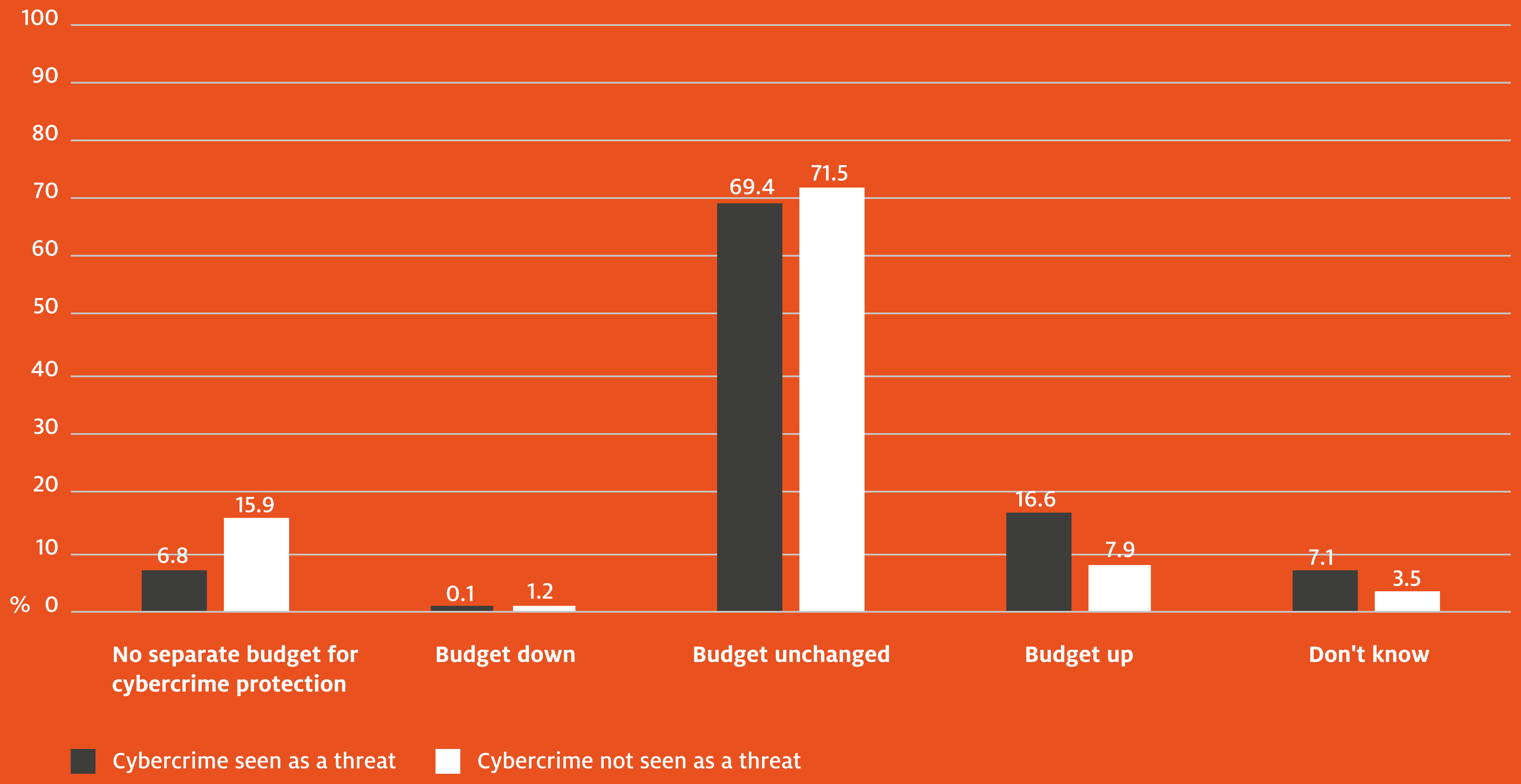


Chart 2: What change, if any, do you expect in your organisation's budget for cybercrime prevention over the next twelve months? (Source GfK, n=512)

3 People are at least as important as systems

Many enterprises treat online security as a technical problem: responsibility is given to the IT department and investment is focused mainly on the protection of their systems. However, people are at least as important as systems. Perhaps more important, since our findings show that many people use log-in methods that they themselves regard as insecure, and use insecure private log-ins in 'secure' business environments. Large numbers also continue to click on insecure links. The good news from our expert panel is that practical security measures can improve an organisation's security almost immediately.

Log-in paradox: convenience versus hassle

Our survey highlighted a mismatch between the popularity of a log-in method and its perceived security. The methods that people use most are the ones they consider least secure. Methods that are viewed as more secure are used less. For example, 57.2 per cent of respondents say that they use social log-ins, such as Google and Facebook, on a daily basis. Yet only 14.4 per cent say that they think such behaviour is safe.

> Chart 3: How well do you think that the following log-in methods protect your privacy?

Similarly, 54.4 per cent of respondents reported using a user name-password combination every day, although only 37.5 per cent see that as a secure way of logging in. iDIN and DigiD – two log-in methods that are perceived as secure – were found to be used less than 'insecure' methods.

According to the panel, the 'log-in paradox' is largely down to convenience: setting up a password only takes a moment, whereas using DigiD involves waiting for an activation code to arrive by post. To win more ground, secure log-ins need to be more user-friendly.

Biometry still not popular

Greater choice of online identities is also needed. Using a secure log-in such as iDIN or DigiD for everything isn't desirable; you might, for example, want to have an anonymous social media-account that isn't linked an identity like that. Biometric log-ins aren't a comprehensive solution to the security-or-convenience conundrum either: using a fingerprint may offer security, but doesn't protect your privacy. What's more, biometric log-ins have yet to really catch on. Only 11 per cent of respondents in our survey said it was their preferred option.

Security isn't a saleable product

The most used (and least trusted) log-in methods are free. Would consumers be willing to pay for a secure, user-friendly alternative? André Koot from Nixu Benelux was unconvinced: "Identity providers don't believe that there's a business case. And if people don't perceive a risk, their willingness to pay for security is bound to be limited." SURFnet's Remco Poortinga-van Wijnen added, "It's an illusion that anyone can offer total security. 'We are secure' can never be a USP."

> Chart 4: What form(s) of cybercrime do you see as the biggest threat(s) to your organisation? (Source GfK, n=512)

‘1234’ still a popular password

For now, logging in with a password of your own choice is an everyday thing. And, being an everyday thing, problems often arise. Despite all the warnings, many people go on using the same – often lamentably weak – password, and use it for multiple accounts. Only 22.7 per cent of our respondents used a very secure password, and just 20 per cent opt for two-factor authentication. Another notable finding: 60 per cent of consumers use insecure Wi-Fi networks to access the internet. Is it fair to say that, in cybersecurity, the user is the weakest link?

User-related vulnerability

Certainly the panel believe that there’s a lot of scope for improving security by addressing user-related vulnerabilities. As Aad van Boven (SecureMe2) said, ‘32 per cent of the cyber alarms we receive are human-initiated. They don’t relate to DDoS attacks, but to cybercrime committed by means of social engineering: phishing and e-mails with ransomware or malware links. We come across a lot of CEO fraud as well, where someone posing as an organisation’s CEO instructs a worker to make a payment to an account controlled by crooks. All of those forms of cybercrime cause serious problems, which can’t be prevented simply by having a good antivirus program.’

> Chart 5: How willing are you to pay for the following? (Source GfK, n=2095)

Security begins with knowledge

The fact that many cybersecurity risks are user-centred isn’t such bad news as it might sound. It implies that people are able to influence their online security. And that behaviour is modifiable. First and foremost, that requires knowledge: people need to know what forms of cybercrime exist, how to recognise them and what to do when they come across them. Awareness training can make personnel more alert and harder to hoodwink. However, there’s a reluctance to invest in this form of protection: our survey found that only 16 per cent of the surveyed businesses arrange for training or instruction. Organisations that do make training available don’t repeat it often enough, the panel believes.

“Awareness training is effective: staff become more cybersecurity-alert, get a better idea of how to deal with phishing e-mails, and point out issues to one another. But many organisations think that you run an awareness session, and then that’s it. In fact, constant repetition is needed for people to take in security advice, bear it in mind and change their behaviour. Awareness training isn’t something you just do and then tick off your list. It’s a process of continuous investment in your organisation. Awareness training tends to be seen as a cost item, when it should be seen as an investment: what you spend is a fraction of what you save by preventing hacks and data leaks.

If you get hit and your computers all go down, preventing everyone from working for a day, the overall cost might add up to, say, 80,000 euros. If you can avoid that by running a course that stops one employee from falling for one phishing scam, you’re hugely in profit. Unfortunately, many businesses don’t see it that way until they’ve been scammed.”

Maria Genova (journalist, writer and speaker)

Shamed into silence

Another factor that the expert panel sees as influential is shame. Businesses that suffer break-ins or fires are open about what's happened, but those hit by cyber-attacks keep the news to themselves.
And individual employees are scared of being seen as stupid, careless or negligent: why on earth did you click on that link? "There's a sense of shame, even though it's universal human fallibility that scammers prey on. And that's hard to protect against," says André Koot of Nixu Benelux.

> *"When a business gets hacked, it's typically hushed up. After all, commercially sensitive information is often involved. Also, customers tend to be wary about using a supplier that's been the victim of cybercrime, fearing that their data may be at risk. The image damage caused by hacking can be seriously problematic for many businesses."*
>
> *Kees Monshouwer, Monshouwer Internet Diensten*

Openness pays

In order to boost cybercrime resilience, the taboo on speaking about incidents needs to be broken. If the subject is discussable, people within the organisation will report incidents or times when they've fallen for a scam. Then you can use regular awareness training to reduce the risk of recurrence. So openness can ultimately make an important contribution to the security of business operations.

Purchasing department needs to be involved

Security isn't exclusively an IT issue; it's also a procurement responsibility. That's because long development lead times mean that many new software systems and other products are already insecure when they come onto the market. By including security in their purchasing requirements, a procurement team can prevent 'rubbish' from entering the organisation. Moreover, when calculating depreciation, a device's technical lifetime should end when its software ceases to be reliable. The expert panel is clear: 'it's still working fine' isn't an excuse. If your product is no longer supported, it needs replacing. Security is therefore an increasingly important aspect of product life cycles, especially with the proliferation of IoT devices.

Start tomorrow

Practical tips for making your organisation more resilient against cybercrime. With thanks to Aad van Boven & Maria Genova.

- Organise interactive awareness training, e.g. 'data leak hide and seek'.
- Show security tips on your organisation's screensaver.
- Promote the use of strong passwords within your organisation.
- Emphasise the importance of updating software promptly.
- Always use two-factor authentication when it's available.
- Connect IoT devices to a separate network from your business systems.
- Disable UPNP on your router and test for open ports.
- Keep security under constant review!

Most popular log-in methods are the least trusted

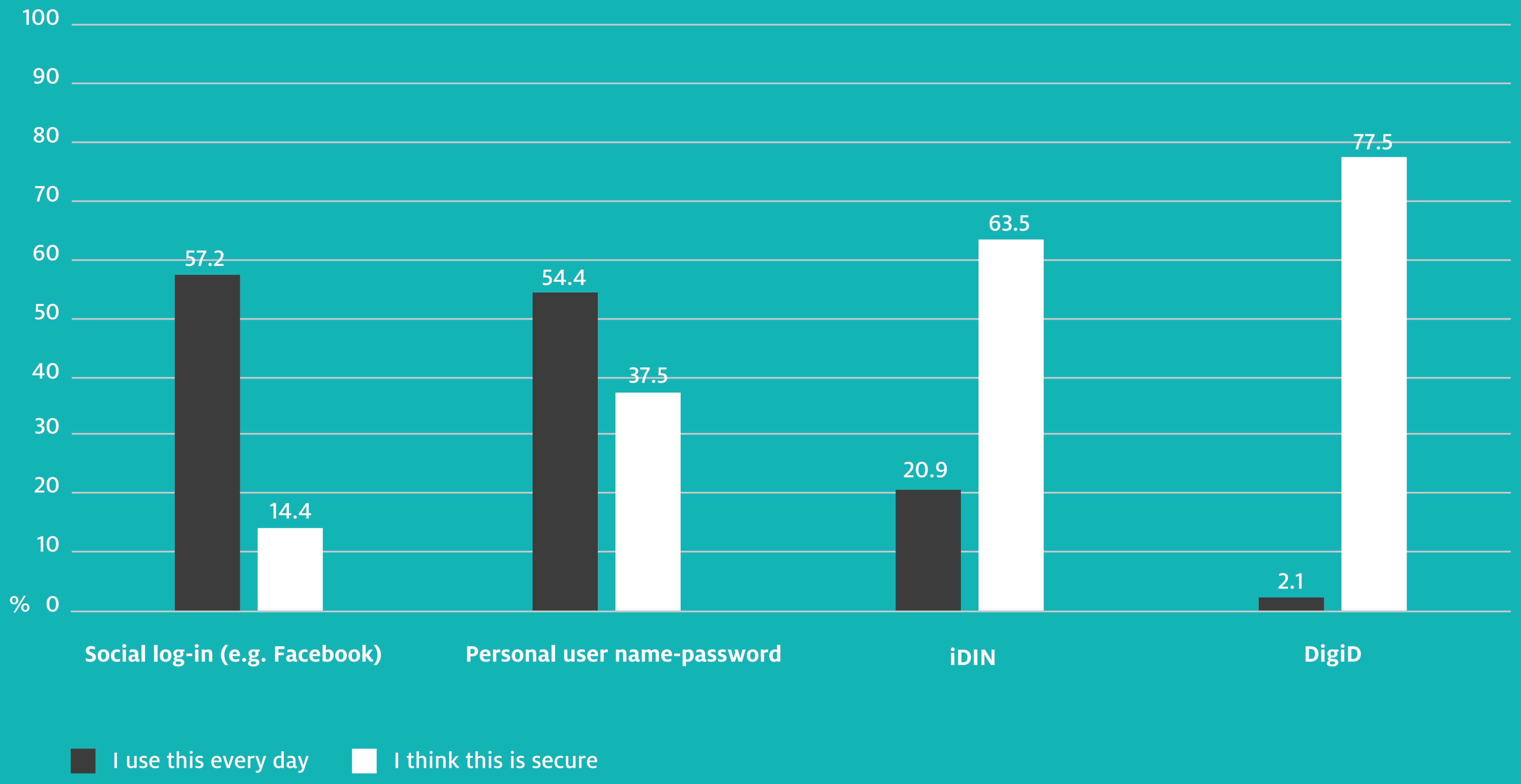


Chart 3: How well do you think that the following log-in methods protect your privacy? How often do you use the following log-in methods? (Source GfK, n=2095)

Focus is on technical threats, especially in small organisations

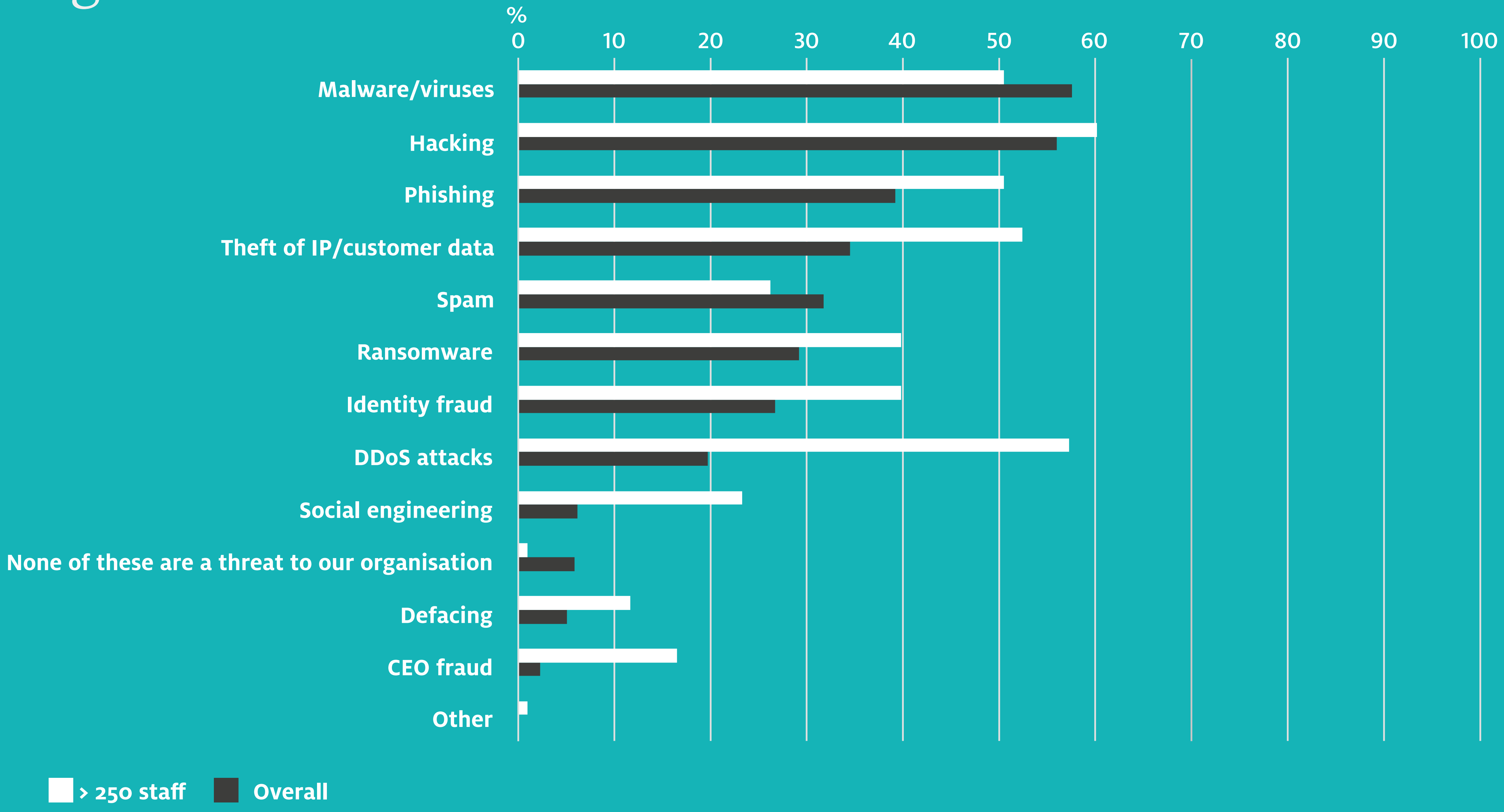


Chart 4: What form(s) of cybercrime do you see as the biggest threat(s) to your organisation? (Source GfK, n=512)

Consumers reluctant to pay for security

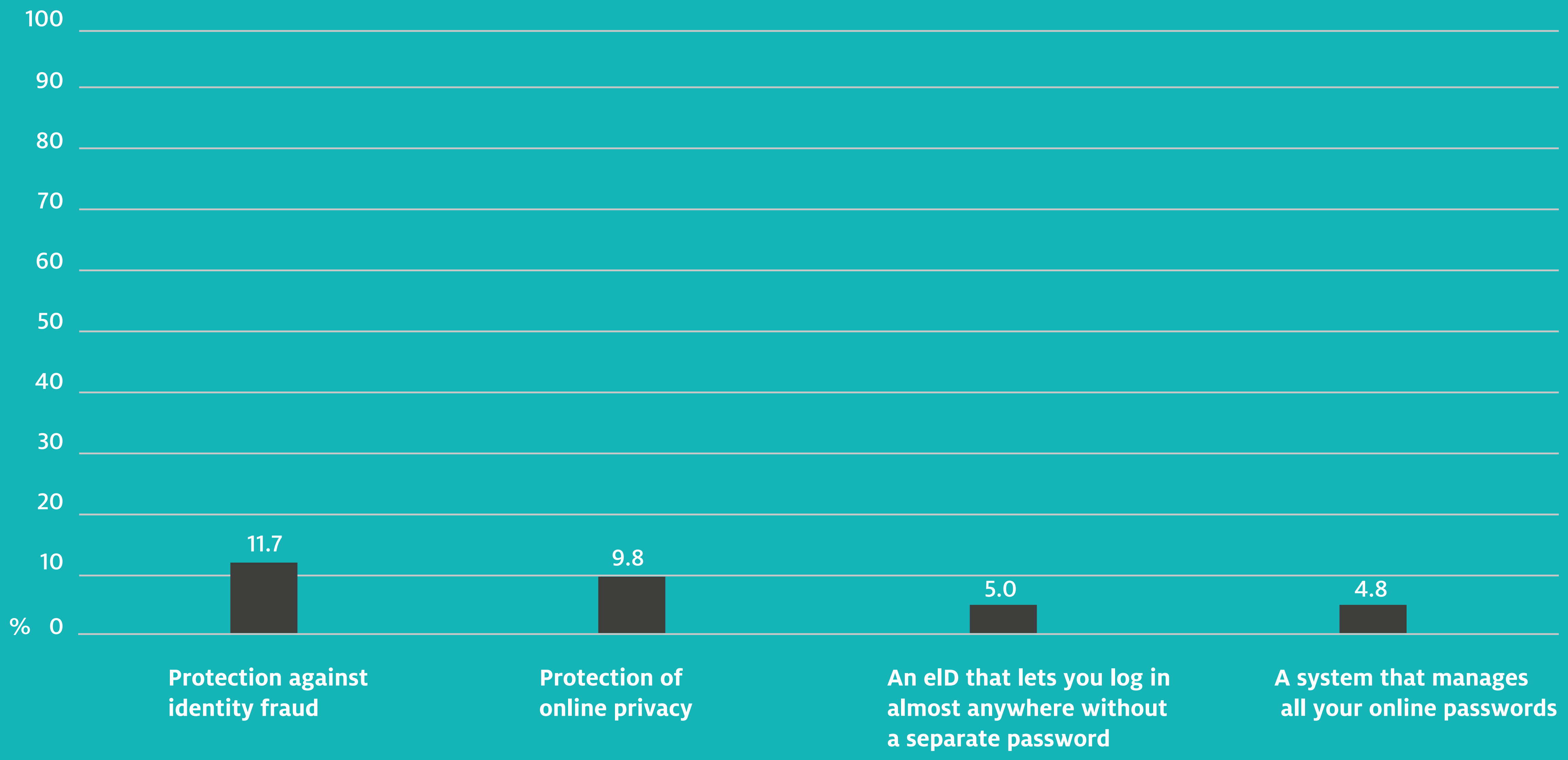
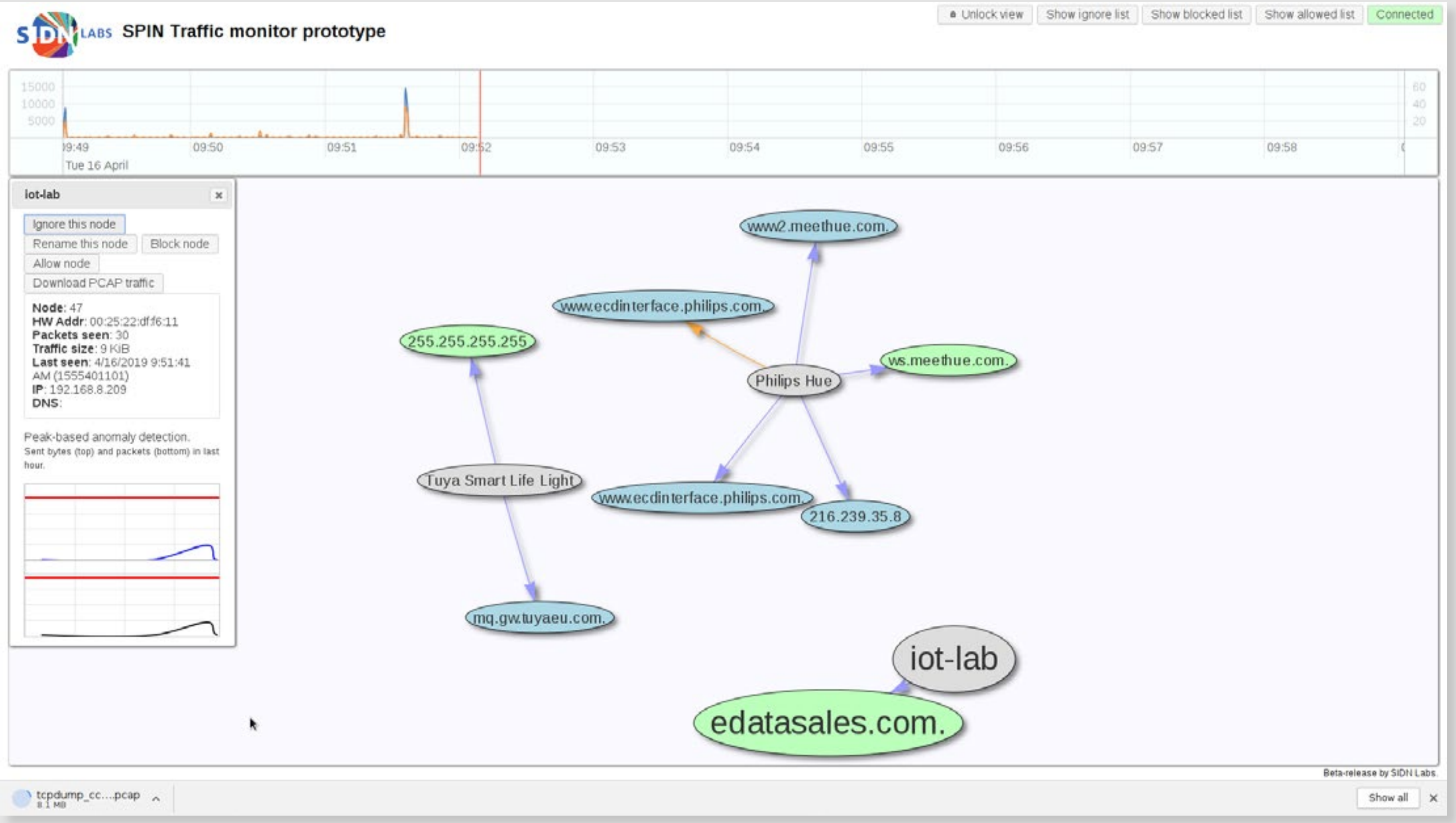


Chart 5: How willing are you to pay for the following? (Source GfK, n=2095)

4 The Internet of Things: how do we make sure it's secure?

Although everyone loves the IoT, people don't know much about it and consequently don't worry much about it either. The expert panel therefore decided to start by defining what the IoT is. The unanimous answer: everything that isn't a computer or server, but is connected to a network via the internet. From Fitbits, through smart lights and coffee machines, to internet TVs: gadgets that everyone nowadays buys on line, preferably as cheaply as possible, often from China. Plug it in, and away you go. Without any idea what the security risks might be. And the exponential growth of such internet-enabled devices has barely begun.

> *"More than half the alarms we respond to relate to IT equipment other than computers and servers. In 90 per cent of cases, we're talking about products bought from ElCheapo, AliExpress or eBay. In December, there's a clear peak: over last year's present-giving season, 11,500 new IoT-devices were added to our home networks. As a society, we're buying everything we can lay our hands on and connecting it to the net. So, it's not altogether surprising that the IoT sometimes gets demonised."*
>
> *Aad van Boven (SecureMe2)*



Node: 47
HW Addr: 00:25:22:df:f6:11
Packets seen: 30
Traffic size: 9 KiB
Last seen: 4/16/2019 9:51:41 AM (1555401101)
IP: 192.168.8.209
DNS:

Peak-based anomaly detection.
Sent bytes (top) and packets (bottom) in last hour.

Figure 1: Real-time overview of devices that connect to the internet via a router (Source: Spin4home.nl)

Most consumers don’t see any great danger

Our survey findings suggest that ignorance leads many people to underestimate the risks. Asked whether the IoT made the internet less secure, most respondents were fairly relaxed: 41.5 per cent replied, ‘slightly less secure’. On the other hand, a sizeable minority (33.7 per cent) saw more reason for concern, replying that IoT made the internet ‘much less secure’. Optimists were few and far between: 3.0 per cent said that the IoT made things ‘slightly more secure’ and just 0.3 per cent responded, ‘much more secure’. Interestingly, a significant number (21.6 per cent) felt that the IoT made no difference. If we count that last group together with those who are only mildly concerned, the conclusion is that more than two thirds of respondents either trivialised the risks or didn’t perceive there to be a risk at all.
> Chart 6: How does the IoT influence security? (Source GfK, n=2095)

Risk increases following purchase

According to the expert panel, buyers put convenience and price ahead of security. Is the answer more security-conscious purchasing? Some panellists argued that the biggest danger with IoT devices was keeping them in use too long. Many consumers don’t realise that a smart light can be a security problem, so they don’t set a password and they’re at risk from day one. However, a more common problem is forgetting to update the software. Or getting careless about it after a while, so that the device becomes less secure with age. And the virtual back door to the home stands ever wider ajar, says Kees Monshouwer: “The big danger is prolonged use. Is everything that’s secure today still going to be secure ten years from now?”

“It doesn’t occur to most people that a dishwasher, webcam or TV needs a password. If they do happen to see something about setting a password on page 5 of the manual, it doesn’t cross their minds that the password will effectively control access to other network devices. Really, the manual should say in bold letters right at the start:
BEFORE CONTINUING, SET A UNIQUE PASSWORD!”

Maria Genova (journalist, writer and speaker)

Who’s responsible?

With such a large predicted data leak from Dutch homes, the question of responsibility inevitably arises. As the Internet of Things gets bigger and bigger, whose job is it to keep us secure: the manufacturers’, the government’s, or ours? Articulated by Aad van Boven, the panel’s answer was in principle clear-cut: “That’s easy: data is leaked by your device. You own it; you’re responsible for it.”

That may be so, according to the letter of the law. Nevertheless, laying all the responsibility in the lap of unaware, unskilled consumers seems a little unfair, and the experts felt uncomfortable about doing that. So are manufacturers responsible? Discussion leader Esther Makaay (SIDN and Connectis) didn’t expect any miracles from that quarter: “Manufacturers and suppliers know that a basic level of ‘product hygiene’ is required, but frequently don’t provide it.”

And that just leaves the government. Reluctantly, the panellists ultimately agreed that the state had a duty to ensure a clear regulatory framework. The new European cybersecurity directive that came into force in March 2019 was therefore welcomed. Amongst other things, the directive provides for the certification of IoT devices sold in Europe. The scheme is initially voluntary, but could be made mandatory in 2023 following a review.

“Many consumers don’t realise how insecure the IoT currently is. In fact, it could hardly be less secure. So the one crumb of comfort is that things can only get better. I think that the government has a role to play in that context. In the end, the government will feel obliged to intervene and define parameters.”

André Koot, Nixu

Majority worried about IoT risks

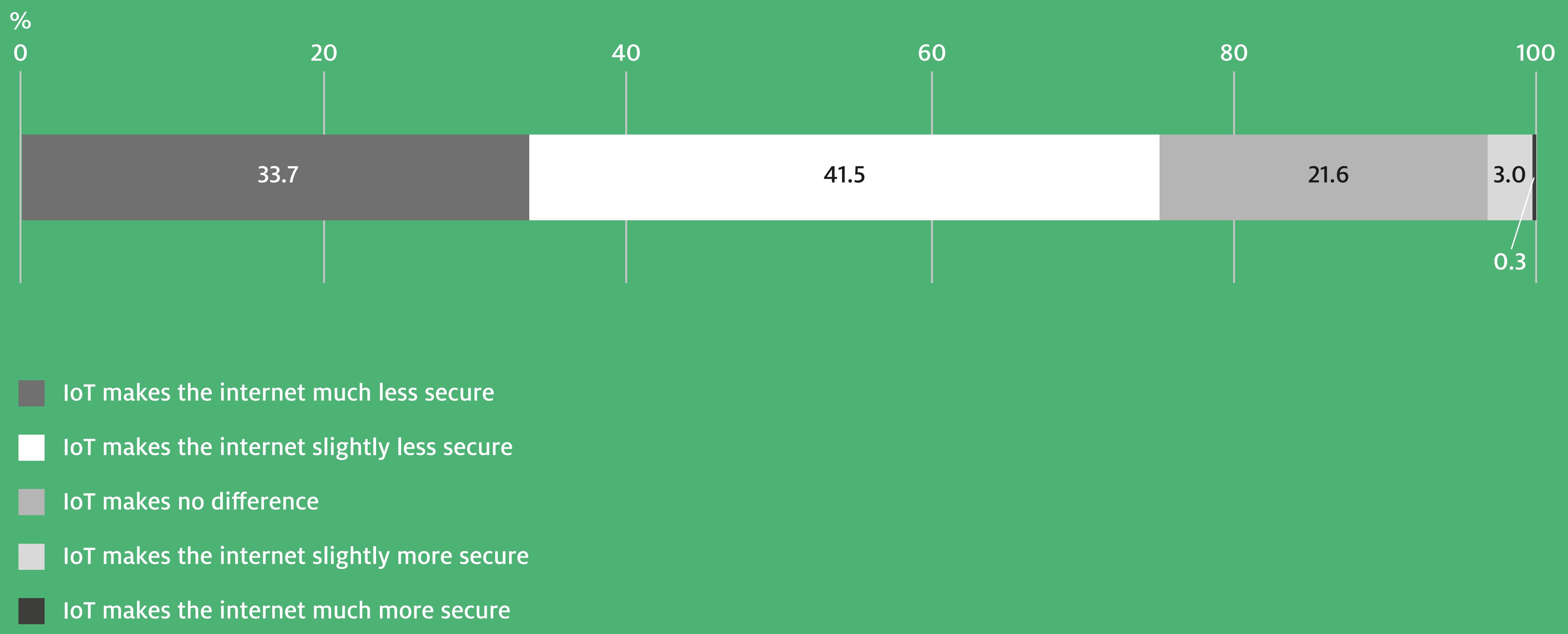


Chart 6: How does the IoT influence security? (Source GfK, n=2095)

5 Who’s responsible for protecting consumers?

So, does online security require a private-sector solution, or a public-sector solution? In other words, should the market resolve the various issues, or the government? The expert panel was unsure, reflecting the mixed and sometimes surprising findings of our survey. And, while we’re on the subject of state intervention: what impact is the GDPR having one year in? Pertinent questions that generated an animated concluding debate.

Rules are pointless without enforcement
Before considering the question of public or private solutions, the panel picked up on another point. The experts were firmly unanimous: legislation has no effect unless it’s enforced. Aad van Boven asserted plainly: ‘Compliance and security are two different things!’

“Security is often seen as an IT problem, and compliance with more rules is seen as providing more protection. That’s wrong on both counts. Online security is a policy issue. It’s a business management issue; it’s about priorities and process design. Because it’s a management-issue, the management often is the issue. CEOs invariably have the most comprehensive system user rights, but often make the biggest mistakes. You can have as many rules as you like, but security is always ultimately about behaviour.”

André Koot (Nixu)

GDPR: good idea that’s become a paper tiger
In the country as a whole, the situation is much like that within an organisation. The GDPR was often cited as an example. The panel endorsed the GDPR’s intentions, but predicted that, without enforcement, people will gradually disregard it.

“The GDPR was briefly hot news, especially in the run-up to introduction, when company boards and managers were being flooded with warnings. However, nearly a year on, interest has waned considerably. SMEs simply make a risk analysis: impact of compliance, high; risk of being punished for non-compliance, zero. So, look the other way and carry on as before. Without enforcement, nothing changes.”

Aad van Boven (SecureMe2)

Lawyers remain alert, ICT people less so
That panel’s analysis is reflected in the survey findings. According to our respondents, the general GDPR-awareness seen last year is now in decline. We asked ICT professionals and lawyers how the GDPR had changed awareness of personal data issues within their organisations. A standout 72.3 per cent of lawyers responded that the new law had influenced awareness ‘a very great deal’. That presumably reflects the legal profession’s inherent inclination to attach importance to laws.
> Chart 7: To what extent has the GDPR influenced personal data awareness within your organisation? (Source GfK, n=512)

Only 2.2 per cent of ICT professionals felt that the GDPR had influenced attitudes ‘a very great deal’, while more than a third (33.8 per cent) attributed ‘quite a lot’ of change to the new law. Nearly half of them (48.8 per cent) suggested that the influence had been ‘a little’. All things considered, the percentage who replied that the GDPR hadn’t influenced awareness at all (15.2 per cent) was quite significant. In summary, on year on from the law coming into effect, ICT people no longer see the GDPR as a pressing issue. By contrast, in line with their role, lawyers retain a keen interest.

The expert panel filled in the picture with real-world examples. Maria Genova pointed to the banking industry:

“The European Central Bank and its Dutch counterpart issued formal security guidelines; they weren’t mandatory, but explained what was and wasn’t allowed under the new regime. The banks paid little attention until the regulators started asking them to demonstrate that they had their security in order. That spurred the banks into action, illustrating that rules aren’t effective until people have an incentive to comply. A box-ticking exercise yields only sham security.”

Maria Genova (journalist, writer and speaker)

Panel unsure

One the final question remained to be answered. Who should have formal responsibility for ensuring online security: the market, which can develop appropriate products and services? Or the government, which can drive security through laws and regulations (if enforced)?

The expert panel’s discussion of e-IDs and the GDPR highlights its ambivalence. The state, author of the GDPR, was seen as the actor with whom the buck stops. However, it was recognised that many security developments are market-generated, without government involvement. The point was also made that the government didn’t have a strong track record of involvement in this field. The feeling was therefore that such projects should be left to the market, where appropriate competence lay.

Young people expect more from the government

The last word goes to our respondents. Who did they feel had primary responsibility for consumers’ online security? Unlike the expert panel, both of our respondent groups attached relatively little responsibility to the market: 12.7 per cent of respondents overall and 18.0 per cent of young people expected the market to take care of security. Overall, most respondents (57.6 per cent) thought that consumers themselves had primary responsibility. The government lagged some way behind, seen as the responsible actor by 29.7 per cent of all respondents. Interestingly, young people were more likely than their elders to expect the government to deliver: 40.8 per cent took that view. In the future, therefore, it seems that the political community will have to get serious about internet security.

> Chart 8: Who do you see as having primary responsibility for consumers’ online security? (Source GfK, n=2095)

Three conclusions emerge:

1. Through the GDPR, the government currently has a positive indirect influence on the online security landscape.
2. However, if the government’s influence is to be truly effective, enforcement is required, of the kind that has had a positive effect in the private sector.
3. The message to the government is: ‘you better shape up’, because the upcoming digital generation sees the protection of online security as a natural task for the government.

GDPR seen as influential mainly by lawyers

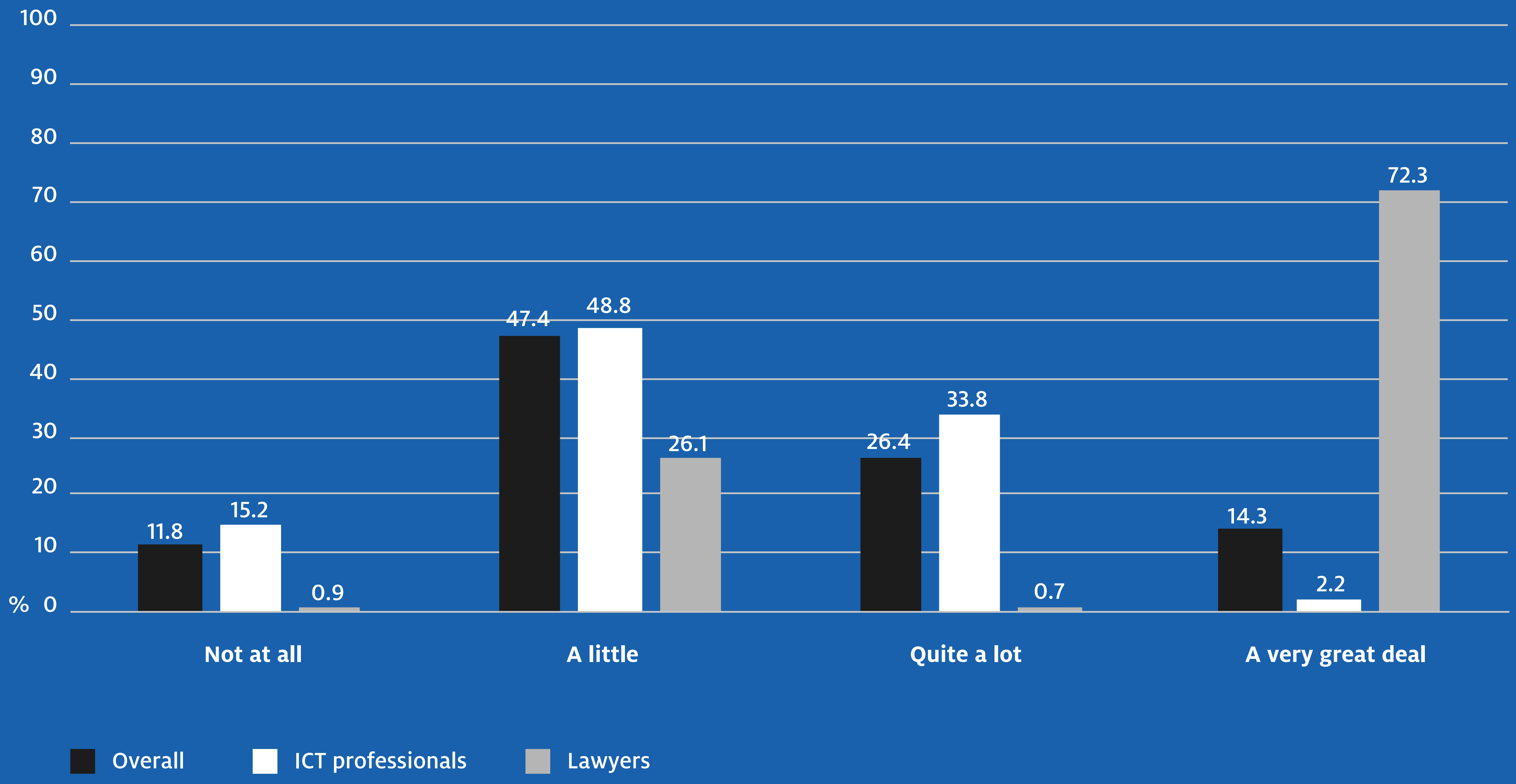


Chart 7: To what extent has the GDPR influenced personal data awareness within your organisation? (Source GfK, n=512)

Young people expect government to play a bigger role

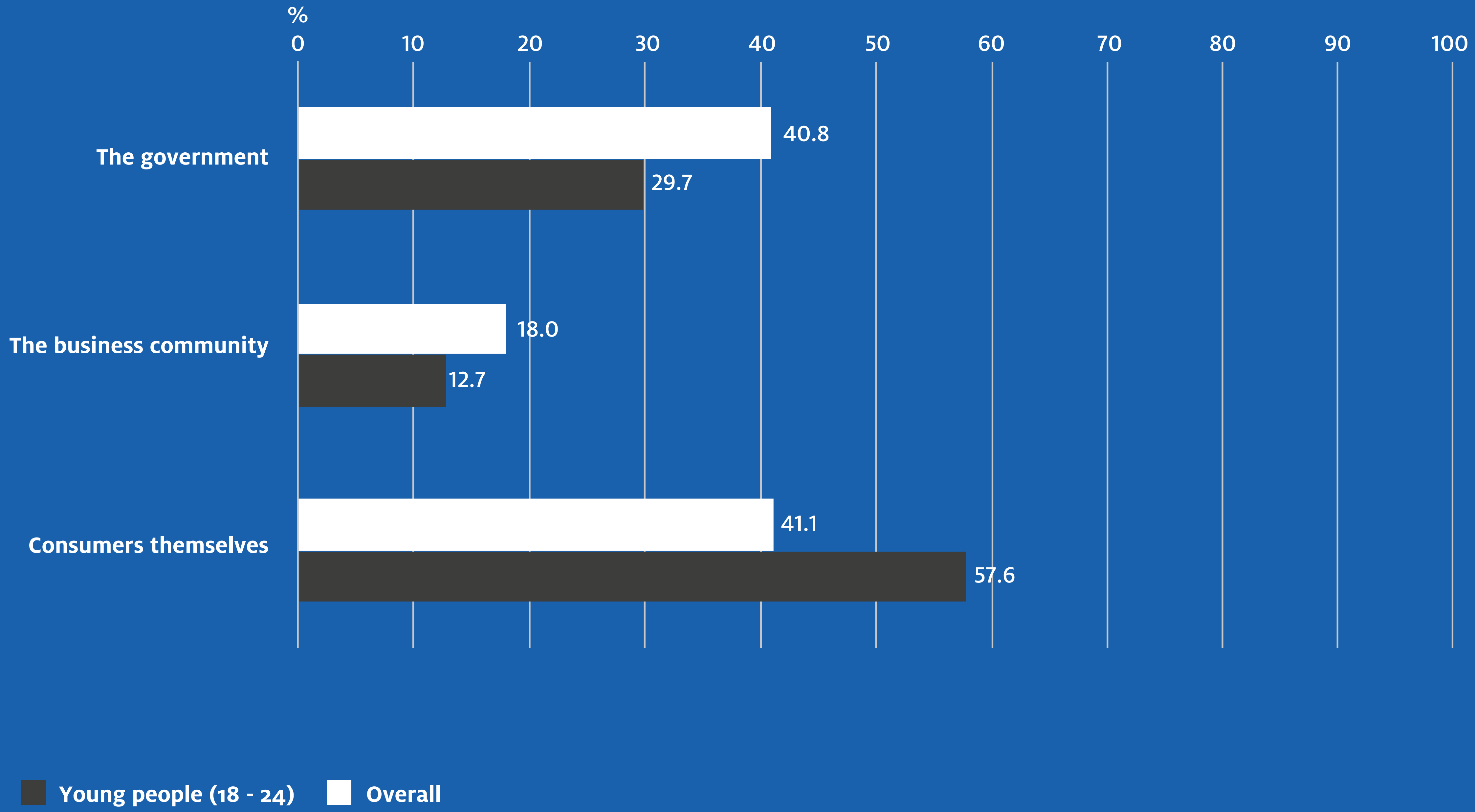


Chart 8: Who do you see as having primary responsibility for consumers' online security? (Source GfK, n=2095)

6 Meet the expert panel

Aad van Boven (SecureMe2) With a background in operational ICT, Aad gained wide-ranging experience between 1990 and 2008.
He worked in various sectors, including energy, telecoms and health care, consistently focusing on the availability, performance and security of ICT infrastructures. He then became self-employed, working mainly as a programme or project manager, kickstarting complex and stalled ICT projects. In 2016, Aad set up SecureMe2, a business that devises high-grade technological solutions to make organisations more resilient in the face of growing cyber threats and against the backdrop of increasingly strict regulatory control.

Maria Genova (author and journalist) As an investigative journalist, Maria has penned several titles, including *Komt een vrouw bij de h@cker (A woman goes to the h@cker)*. That book's success has led to many invitations to speak on identity fraud, privacy and information security. She has given hundreds of interactive talks to audiences in all sectors of the economy, driven by her mission: to help as many people and businesses improve their resilience to increasing digital hazards.

André Koot (Nixu) As well as being a very experienced information security consultant, André specialises in identity management and authorisation control, which he firmly believes should be treated as distinct fields. He also pursues a personal crusade against abuse of the word 'cyber'.

Esther Makaay (Connectis) Esther is an internet technology expert specialising in digital identities. At Connectis, she develops eID innovations. Esther's many fields of expertise include trust frameworks, digital identities and eID schemas, DNS(SEC) and (new) top-level domains.

Kees Monshouwer (Monshouwer Internet Diensten) Kees is an SIDN registrar and a member of the Registrars' Association Technical Committee. In short: an experienced hosting industry entrepreneur. In recent years, he has frequently advised SIDN and its registrars on the implementation of DNSSEC and other open standards with the aim of reinforcing internet security.

Remco Poortinga-van Wijnen (SURFnet) After studying Electric Engineering (University of Twente, 1997), Remco began as a software developer at Ericsson. From there, he moved to the Telematica Institute, working as a research engineer and in other roles. With his extensive knowledge of middleware, federative identity management, software architecture, and security and project management, he was recruited by SURFnet in 2008. Remco now heads up SURFnet's Security & Privacy Team, which is responsible for the innovation and delivery of services within the security and privacy domains.

Aad van Boven, Kees Monshouwer Remco Poortinga-van Wijnen, Esther Makaay, Maria Genova and André Koot.

Colophon

This document summarises a research report compiled by GfK for SIDN and Connectis.

Contributors:

GfK
Henk Delfos – Industry Lead
Ewout Witte – Business Analist

SIDN
Michiel Henneke – Marketing Manager
Christiene Bouwens – Marketing Manager
Marnie van Duijnhoven – Communications Manager

Connectis
Ellen Breugem - Marketing & Communications Manager
Esther Makaay - Business & eID Analyst

Tekstwerf
Rosanne Koppert - Copywriter
Joa Smits – Copywriter

G & J Barker Translations
George Barker - Translater

Questions about the research may be mailed to
communicatie@sidn.nl

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

Connectis
PO Box 975
3000 AZ Rotterdam, The Netherlands
Weena 327-329
3013 AL Rotterdam, The Netherlands
T +31 (0)88 012 02 22
https://connectis.com