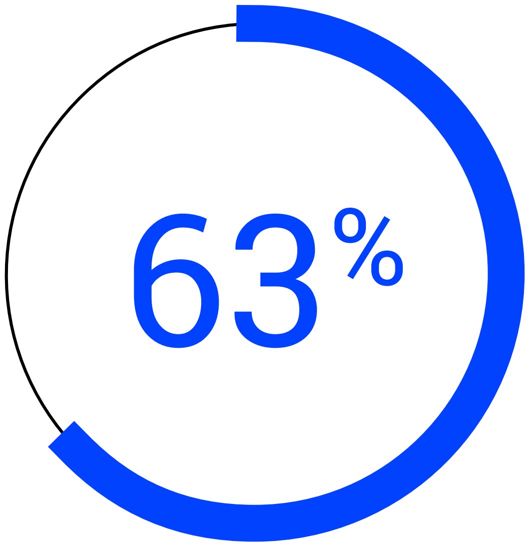
Bitdefender®

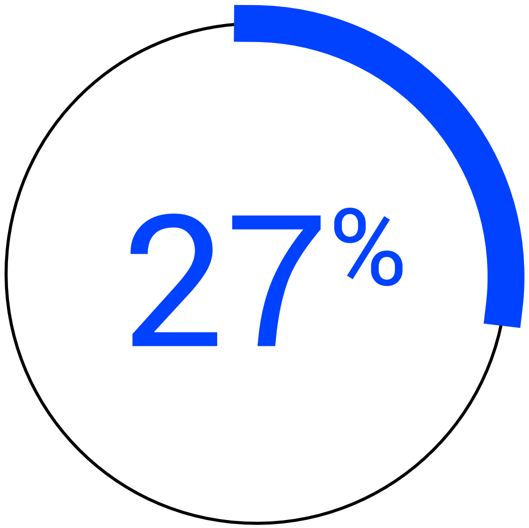
10 in 10

2020

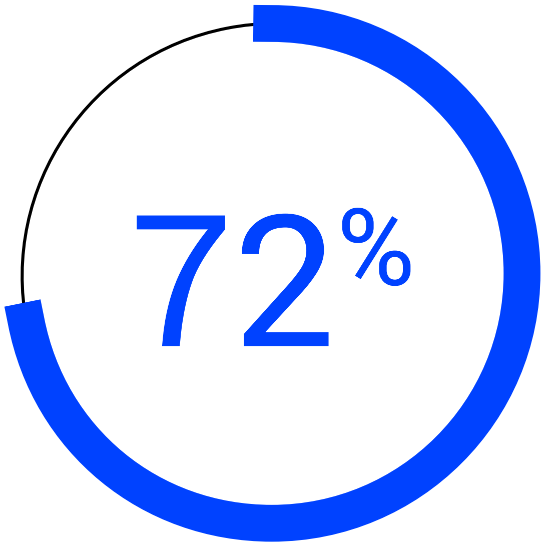
INTRODUCTION



believe that the **state of cyberwarfare** is a threat to their organisation



of companies **don’t have a strategy** to protect against cyberwarfare



believe that there **is a need for a more diverse skill set** in cybersecurity

INTRODUCTION

Today businesses and the technologies within them are in a constant state of flux. At the same time, change in business is being met with an increasingly complex and rapidly evolving cybersecurity landscape — with the risks of threats such as ransomware and cyberwarfare on the rise.

Infosec professionals are undoubtedly feeling the effects and pressure of this constant state of change in cybersecurity requirements. The research reveals that there has never been a more important time to invest in cybersecurity, and that infosec professionals are starting to understand that there is a need for a more holistic approach to cybersecurity. Instead of just looking for ways to avoid risk, and throwing money at the challenge, infosec professionals need to reconsider how, as an industry, it's time to change the way we communicate to the wider business about cybersecurity — if we hope to maintain trust and build understanding. This is especially true when it comes to threats such as ransomware, where most infosec professionals believe there will be a significant increase in attacks over the next 12-18 months.

"Infosec professionals are in the process of witnessing a shift in how the industry operates, with a greater business and media focus on everything from hacks through to state-sponsored cyber warfare, there has never been a more important time for businesses to get it right.

Bogdan Botezatu, Director of Threat Research at Bitdefender

INTRODUCTION

The constant state of change and rapidly evolving cybersecurity landscape, has led us to conduct the 10 in 10 Study — a comprehensive piece of independent research — looking at what factors will most impact security success in the next decade.

The research has explored the specific expectations organisations have when it comes to security, and with the help of third parties, examined what security teams would want to do if they had more time, more money and company cultures that embraced and supported cybersecurity. The research covers these core areas:

Communication: The impact the way the industry communicates has on business, it's expectations and willingness to support cybersecurity

Cyberwarfare: Painting a picture of how big the threat of cyber warfare is, and exploring the current investment in protecting against its impact

Skills diversity: Identifying what the skills deficit currently is, and how it is affecting cybersecurity provisioning

Ransomware: The rise and fall, and rise again of ransomware — and why this is the case

IoT devices: Highlight how, and why, IoT devices are rising in popularity, and why current security standards are no match to it

> “**The Bitdefender *10 in 10* Study, takes into account the opinion of 6,724 infosec professionals in large organisations across the US, EMEA and APAC. It shows that many infosec professionals have the same concerns they did five years ago, but that there are also some new players in the mix. The rise of IoT devices and increasing worry around cyberwarfare might be recent concerns, but they are certainly front of mind for infosec professionals and the impact of not addressing them is likely to cause widespread damage. Though there is some increase in understanding of key cybersecurity issues, there are concerning gaps in knowledge when it comes to new threats, as well as fragmentation between the speed in which businesses are needing to adapt vs their cybersecurity protection.**
>
> **Bogdan Botezatu, Director of Threat Research at Bitdefender** ”

COMMUNICATION IS KEY

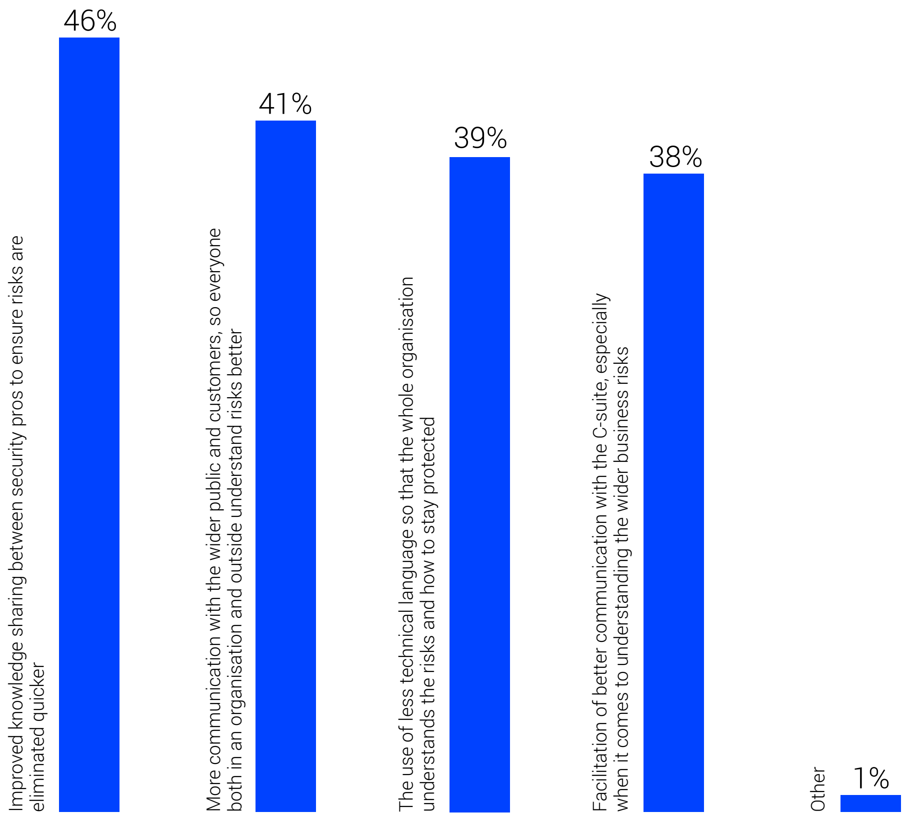
Cybersecurity is complicated and infosec professionals often speak in a language that only those with a deep knowledge of security will understand. As such, businesses leaders and consumers are often left lost in a sea of information and industry jargon. These results highlight that unless the industry takes note and learns to better communicate, it doesn't matter what tools are available, there will always be gaps — which cybercriminals will be well placed to fill.

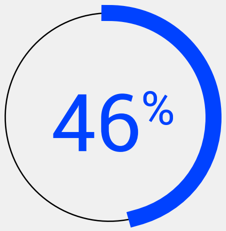
COMMUNICATION IS KEY

Breaking down the barriers

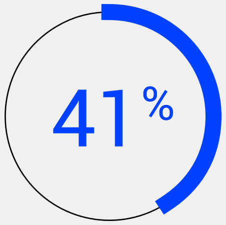
Infosec professionals believe change is needed when it comes to communicating in the future

What do you think needs to change most in terms of how the security industry communicates in the future?

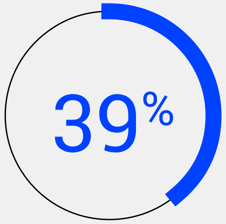




46% of infosec professionals believe that improved knowledge sharing between infosec professionals needs to change the most, in terms of how the security industry communicates in the future. This will ensure risks are eliminated quicker.



41% also believe that in the future, more communication with the wider public and customers is needed so everyone, both in an organisation and outside, better understand the risks.



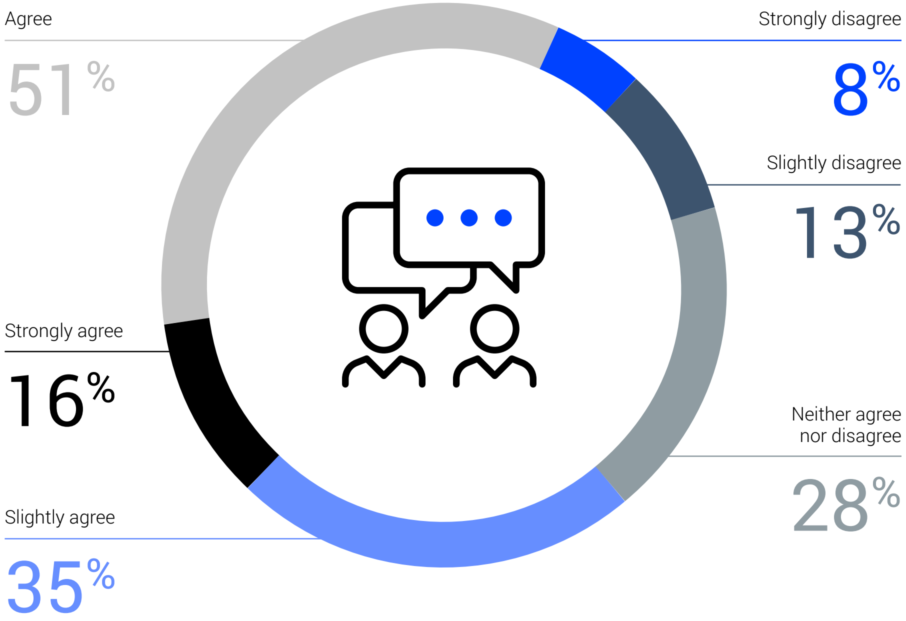
Overall, 39% believe using less technical language would help the industry communicate better, so that the whole organisation could understand the risks and how to stay protected.

COMMUNICATION IS KEY

Breaking down the barriers

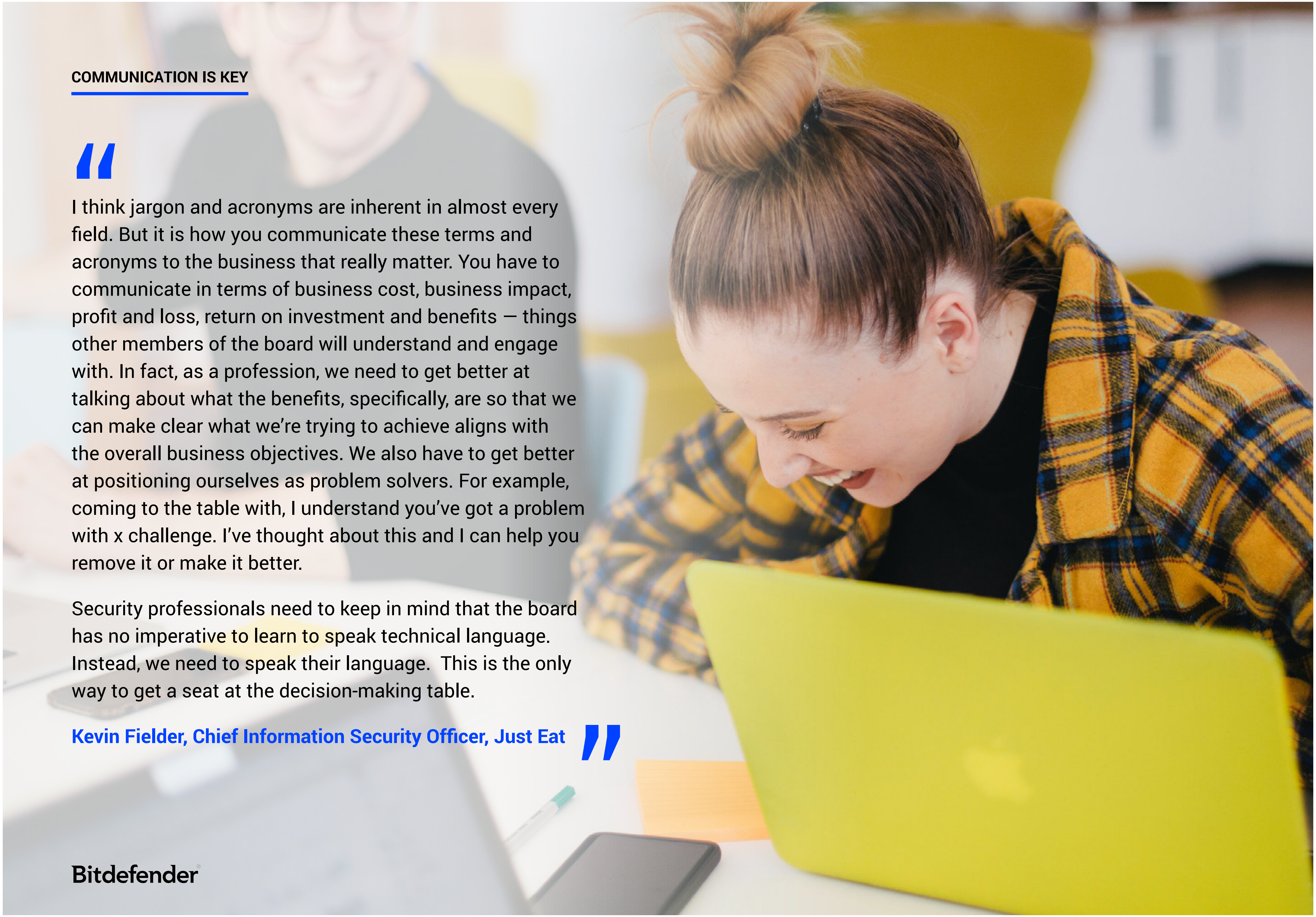
Infosec professionals believe change is needed when it comes to communicating in the future

Please indicate to what degree you agree or disagree with the following statement: The way we communicate cyber risk to the business needs to change dramatically if we want increased investment



51% of infosec professionals agree that in order to increase investment in cybersecurity, the way that they communicate about security has to change dramatically.

This number jumps up to **55% amongst CISOs and CIOs** — many of whom have a seat at the most senior decision making table in their organisations.



COMMUNICATION IS KEY

> I think jargon and acronyms are inherent in almost every field. But it is how you communicate these terms and acronyms to the business that really matter. You have to communicate in terms of business cost, business impact, profit and loss, return on investment and benefits — things other members of the board will understand and engage with. In fact, as a profession, we need to get better at talking about what the benefits, specifically, are so that we can make clear what we're trying to achieve aligns with the overall business objectives. We also have to get better at positioning ourselves as problem solvers. For example, coming to the table with, I understand you've got a problem with x challenge. I've thought about this and I can help you remove it or make it better.
>
> Security professionals need to keep in mind that the board has no imperative to learn to speak technical language. Instead, we need to speak their language. This is the only way to get a seat at the decision-making table.

Kevin Fielder, Chief Information Security Officer, Just Eat

CYBERWARFARE

The threat of cyberwarfare is a concern for infosec professionals, and there is a need to encourage business leaders to understand the risks and the extent of damage that can be done. With cyberwarfare garnering more and more media attention, it’s never been more important to address the threat.

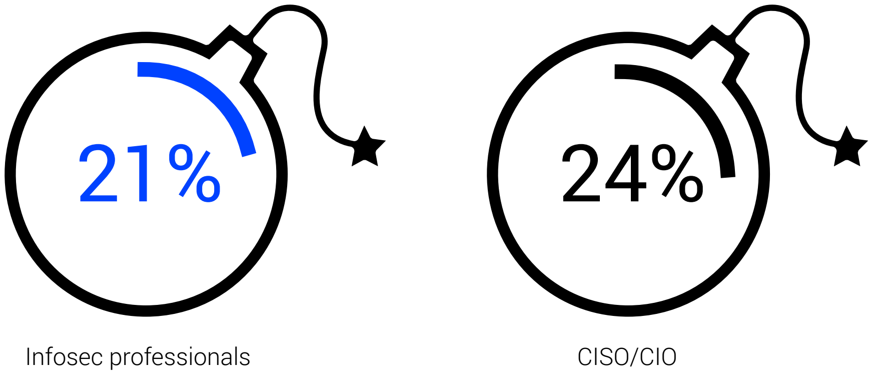
CYBERWARFARE

Cyberwarfare is a concern for businesses

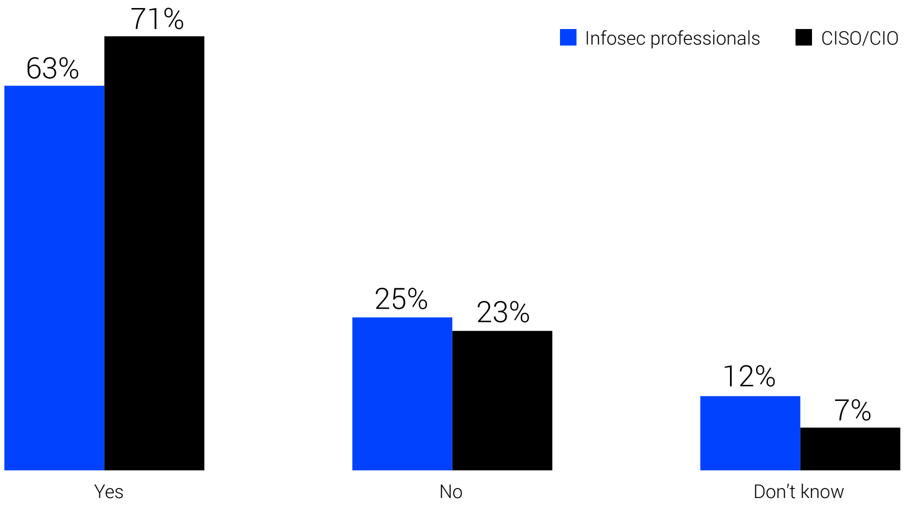
The C-Suite is most concerned about their business being susceptible to a cyberwarfare attack

Over a fifth of infosec professional (21%) said that cyberwarfare / nation state attacks have been the most challenging issues / topics / threats / subjects for business leaders to understand over the last few years. However, this number jumps to almost a quarter of those in CISO and CIO positions (24%).

Please indicate to what degree you agree or disagree with the following statement: The way we communicate cyber risk to the business needs to change dramatically if we want increased investment



Do you believe that state cyberwarfare is a threat to your organisation?



A significant portion of CISOs and CIOs believe that the state of cyberwarfare is a threat to their organisation (71%). This is a figure however falls to 63% amongst those in the infosec professionals.

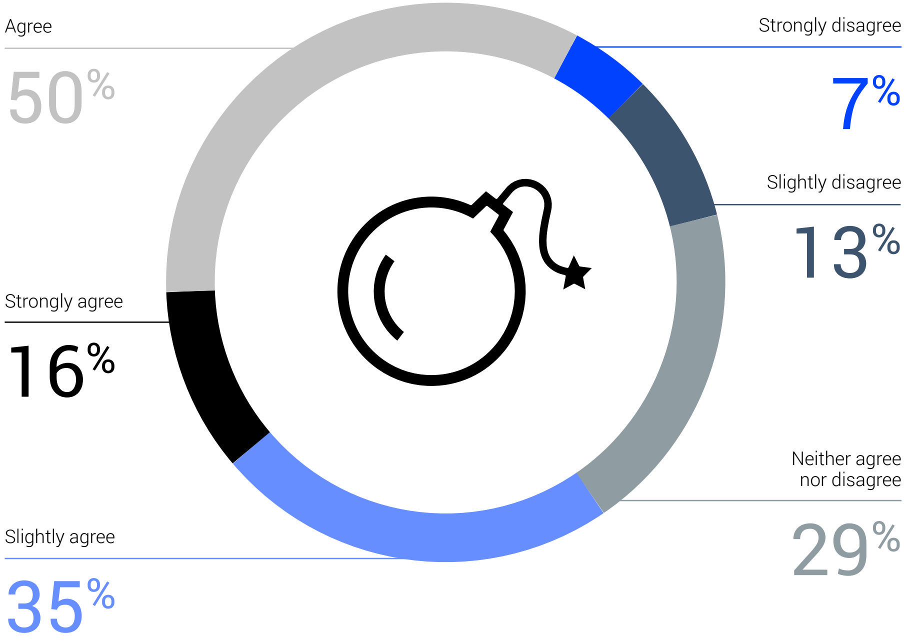
CYBERWARFARE

Beyond an internal concern

Cyberwarfare will impact customers and the wider economy, outside of just business

Half of infosec professionals (50%) expect the increase of cyberwarfare will be detrimental to the economy within the next 12 months.

Please indicate to what degree you agree or disagree with the following statement: "Instances of cyberwarfare will increase in the next 12 months, and it will be to the detriment of the economy"



What do you believe would be the most critical information lost and/or consequences faced if your company became the target of cyberwarfare?

37%	Loss of customer information
33%	Loss of financial information
31%	Loss of employees' personal information
31%	Reputational damage
30%	Business interruptions
27%	Loss of intellectual property
26%	Loss of revenue or markets share
24%	Loss of research about new products/services
21%	Legal fines
17%	Loss of C-Suite/executive jobs

Overall, infosec professionals listed that loss of customer information (37%) would be the biggest consequence if their company was to become a target of cyberwarfare, valuing it over loss of financial information (33%), reputational damage (31%) and loss of revenue/market share (24%).

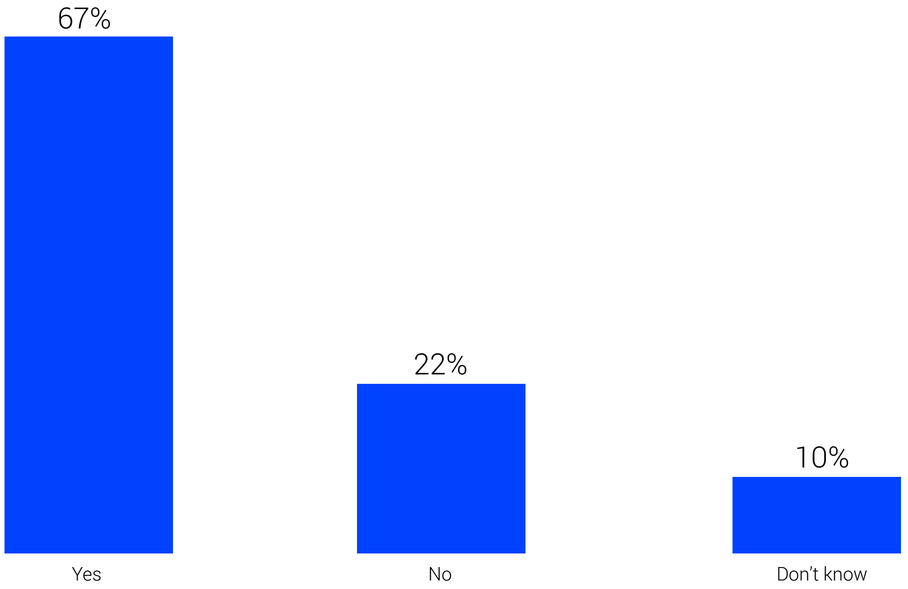
CYBERWARFARE

Preparation, preparation, preparation

As ever, preparation is key when it comes to fighting against any threat to security

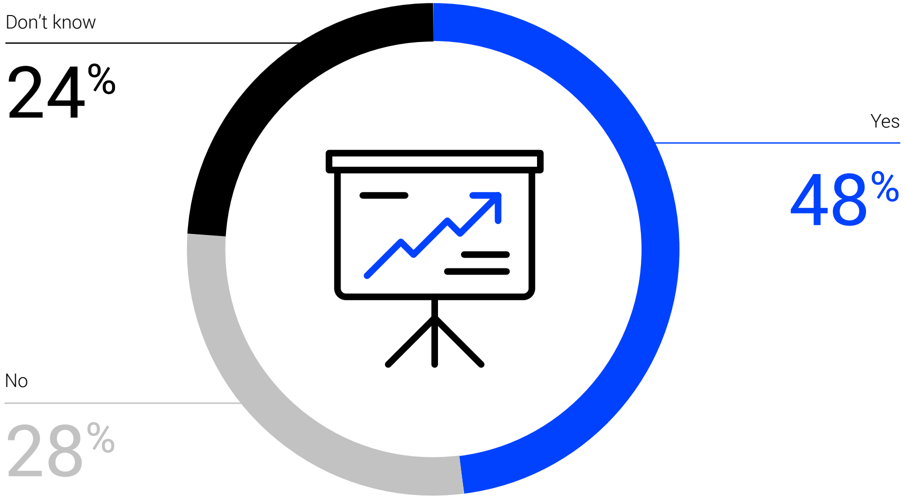
Despite two thirds of organisations having a specific strategy in place to protect against cyberwarfare (67%) more than a fifth (22%) don't.

Does your organisation have a specific strategy in place to protect against cyberwarfare?



Of those that don't have a strategy in place, 48% of infosec professionals, and 51% of CISOs/CIOs, believe that businesses will need a specific strategy in place to protect against cyberwarfare in the next 12-18 months. Only 24% of infosec professionals don't know whether they will or not need a strategy.

Do you believe the business will need a strategy in the next 12-18 months?

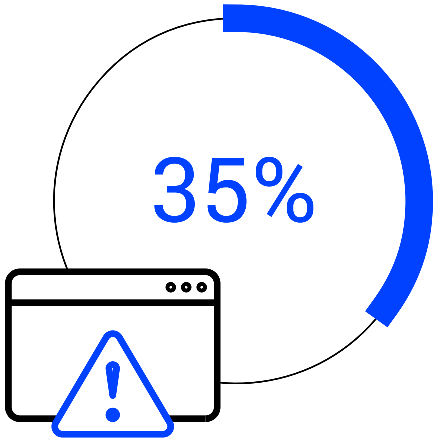


CYBERWARFARE

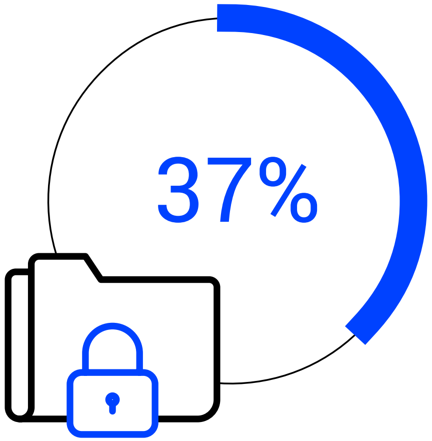
The key to combating cyberwarfare

Although cyber security is a concern for many infosec professionals, what can be done to better protect businesses?

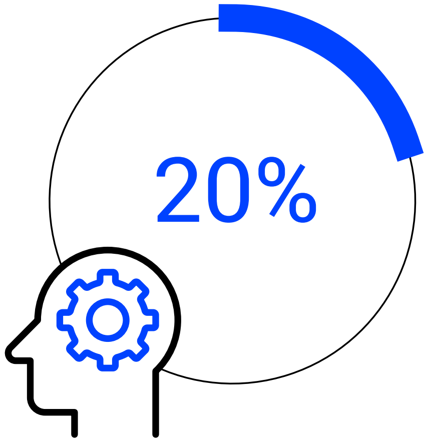
According to over a third of respondents (35%), a better understanding of the threat landscape (35%) or investing in more cybersecurity defenses (37%) are the best ways for businesses to combat cyberwarfare. In addition, 20% of infosec professionals believe that increased neurodiversity in the sector will help combat cyberwarfare.



Better understanding of the threat landscape



Investing in more cybersecurity defenses



Neurodiversity in the sector will help combat cyberwarfare

CYBERWARFARE

The key to combating cyberwarfare

What, in your opinion, is the best way for businesses to combat cyberwarfare?

	All respondents	UK	US	Australia/New Zealand	Germany	France	Italy	Spain	Denmark	Sweden
More investment in cybersecurity defences both from government and the private sector	37%	35%	36%	36%	37%	34%	38%	44%	30%	43%
A better understanding of the threat landscape	35%	33%	35%	40%	41%	33%	33%	28%	34%	42%
More cooperation between public and private sector organisations as it relates to cybersecurity	31%	29%	30%	36%	28%	29%	35%	34%	33%	33%
Better intel within national security that can feedback threats to businesses	25%	26%	26%	29%	25%	24%	24%	24%	23%	24%
Better intel within law enforcement that can feedback threats to businesses	25%	26%	26%	29%	25%	24%	24%	24%	23%	24%
A higher rate of outsourcing security services to MSSP and SOC	24%	24%	25%	24%	21%	22%	22%	27%	20%	18%
More help from government in terms of funding and education	24%	24%	25%	24%	21%	22%	22%	27%	20%	18%
Increased neurodiversity in the sector	24%	24%	25%	24%	21%	22%	22%	27%	20%	18%

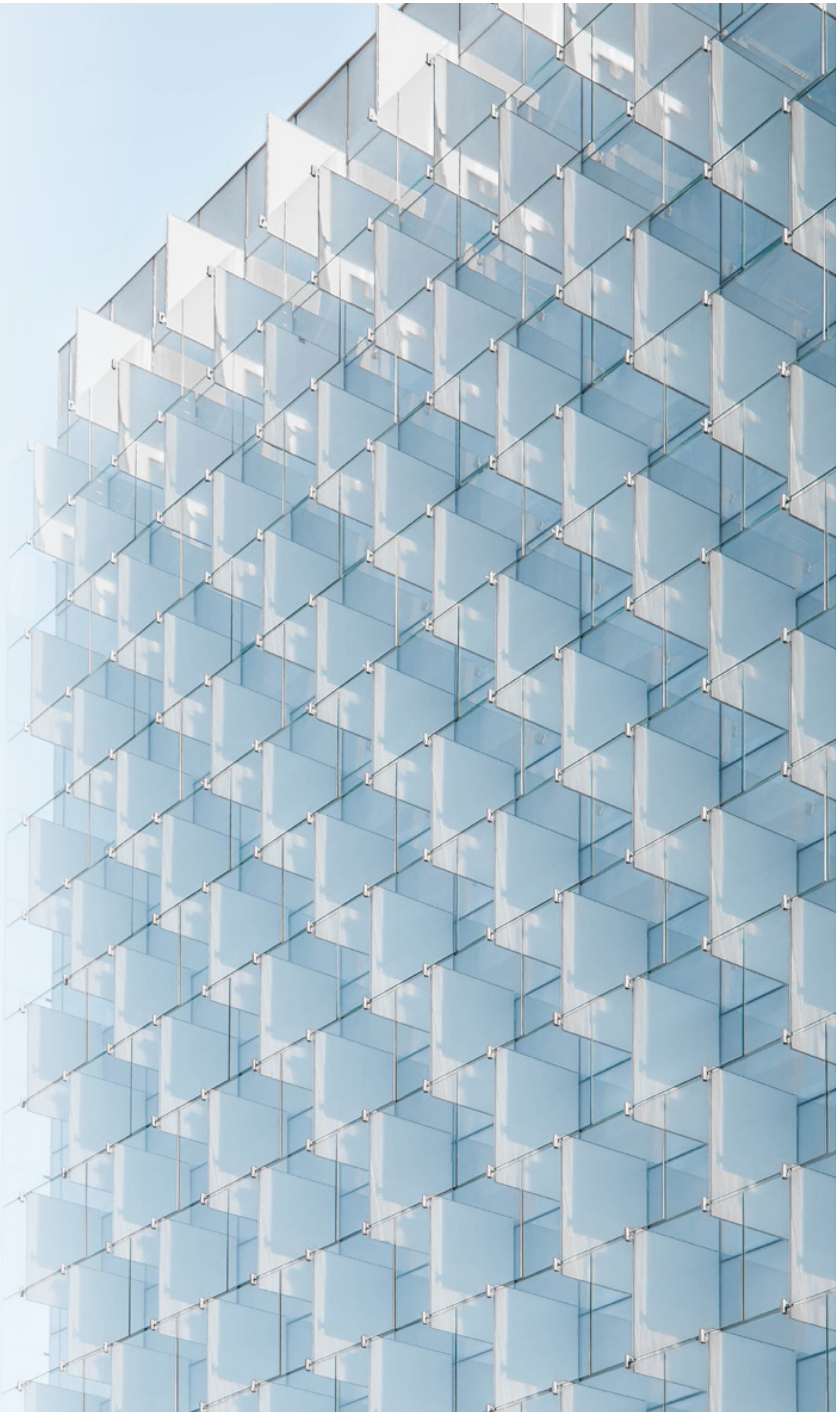
> “The reason that 63% of Infosec professionals believe that cyberwarfare is a threat to their organisation is easy. Dependency on technology is at an all time high and if someone was to take out the WiFi in a home or office, no one would be able to do anything. This dependency wasn’t there a few years back, it wasn’t even as high a few months back. This high-dependency on technology, doesn’t just open the door for ransomware or IoT threats on an individual level, but also to cyberwarfare which can be so catastrophic it can ruin economies. The reason that nearly a quarter of infosec pros don’t currently have a strategy to protect against cyberwarfare is likely because of complacency. Since they haven’t suffered an attack, or haven’t seen on a wide scale the damage that can be done, they haven’t invested the time in protecting against it.
>
> **Neeraj Suri, Distinguished Professorship and Chair in Cybersecurity at Lancaster University**”

“

Cyberwarfare is interesting because unlike kinetic weaponry — which is used in traditional warfare — it hasn’t become more precise. It’s actually become harder to put boundaries around and to control. Think back to Stuxnet. It had a very specific target, a very specific intention, and was successful in that attack. But then, the code of Stuxnet got out and it has now been used in many other subsequent forms of attack. So that goes to show how something that is born of a nation-state attack can then morph and be used in other kinds of attacks. I think that’s a lot of the reason why organisations and professionals now understand that they can be caught up in cyberwarfare in many different layers, for many different reasons.

Social engineering is also something to be aware of in terms of cyberwarfare — it’s much harder to predict and harder to defend against. Take the US election for example, where there has been alleged involvement from Russia, no one really saw it coming in the way that it took place and exploited social media to such an extent. The way that social engineering was, and will be, used can also cause disruption. Mass social engineering, and disinformation, can and will manipulate the way people think and perhaps even act.

Dr Jessica Barker, Socio-Technical Lead at Cygenta, Chair of ClubCISO ”



SKILLS DIVERSITY

It’s no secret that cybersecurity struggles with not having enough skilled workers. But how is the current landscape changing and is an increase in skills diversity likely to happen over the next five years?

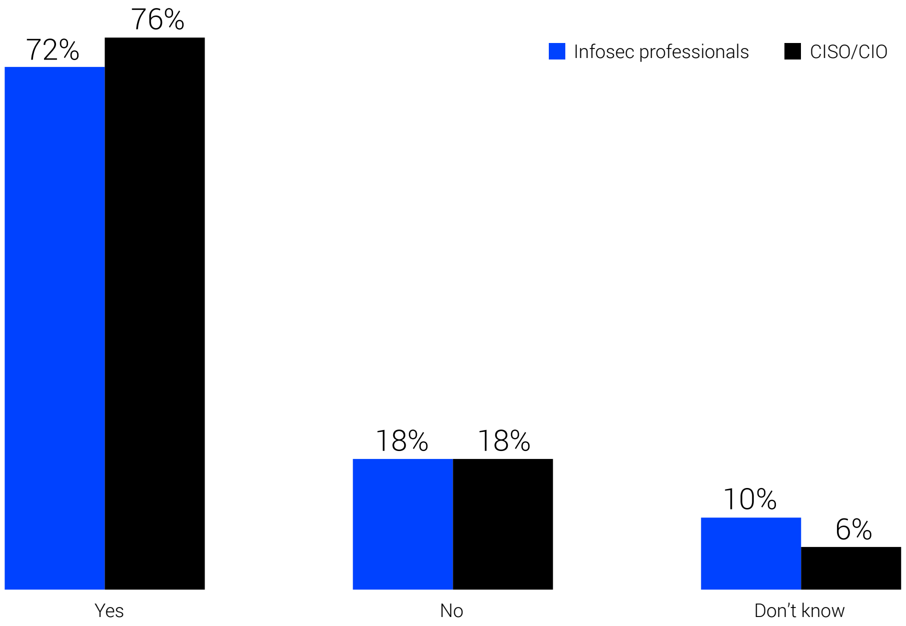
SKILLS DIVERSITY

Diversity in the workplace is still a concern

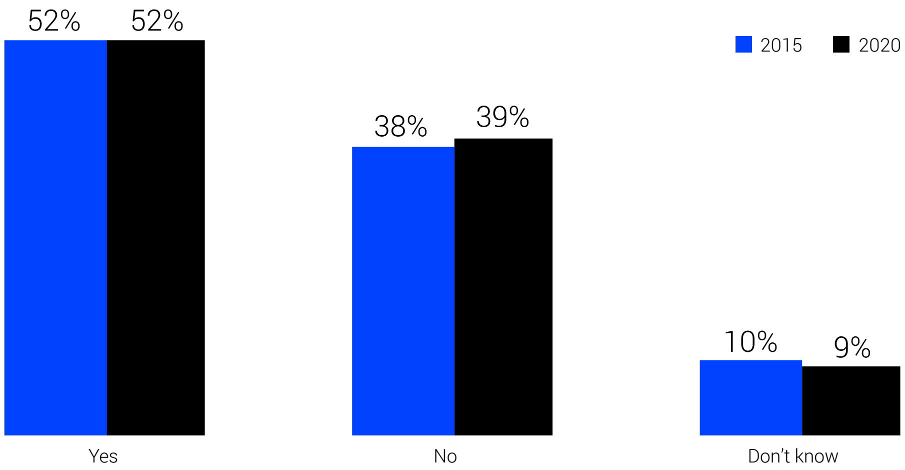
Having a diverse team has been a focus for a long time, but how have things changed over the last five years?

76% of CISOs/CIOS, and 72% of infosec professionals, believe that there is a need for a more diverse skill set among those tackling cybersecurity tasks.

Do you believe that there is a need for a more diverse skill set in cybersecurity?



Please indicate whether you would have agreed or disagreed with the following statements in 2015 and 2020: There is lack of diversity in cybersecurity — and it's of concern.



Yet, in 2015, 52% would have agreed that there is a lack of diversity in cybersecurity and it is a concern. Five years later, in 2020, this remains exactly the same. This is also interesting as 40% say that the cybersecurity industry should reflect the society around it to be effective.

SKILLS DIVERSITY

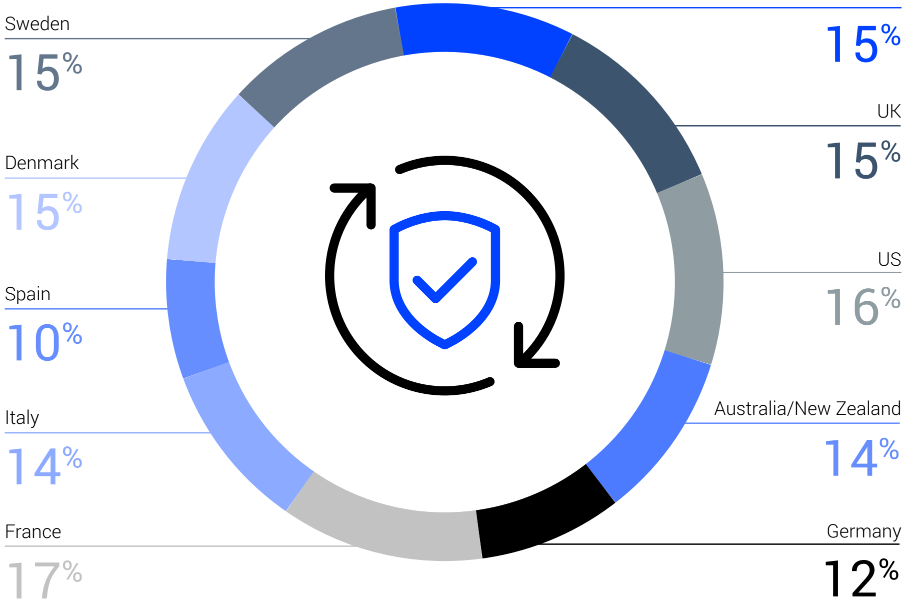
The benefits of a diverse team

Infosec professionals believe there are many benefits when it comes to having a diverse cybersecurity team

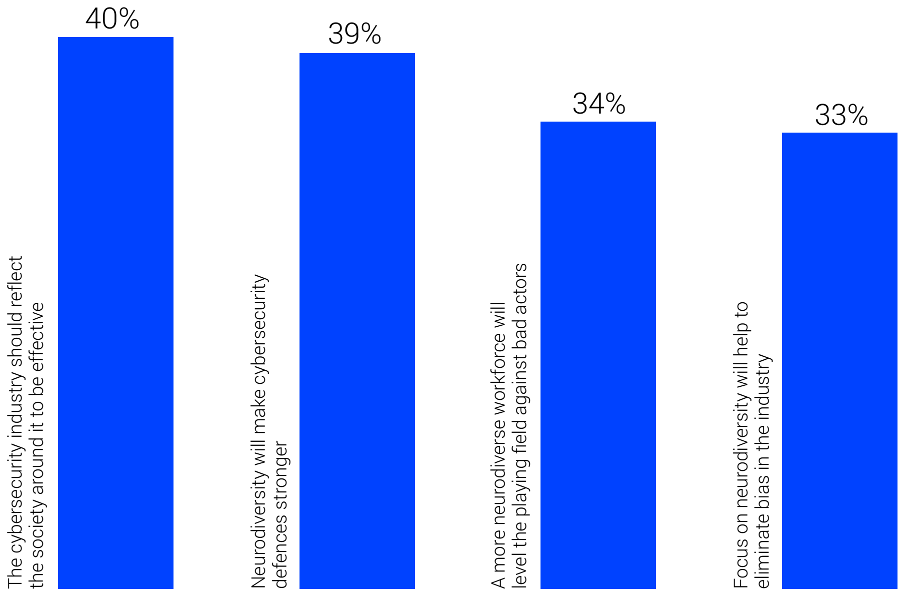
15% of infosec professionals believe that the biggest development in cybersecurity over the next 12-18 months will be the skills gap increasing and a further 20% believe that increased neurodiversity in the sector will help combat cyberwarfare.

38% also cited the fact that neurodiversity will make cybersecurity defences stronger, 34% said a more neurodiverse workforce will level the playing field against bad actors, and 33% said neurodiversity will help to eliminate bias in the industry.

In your opinion, what will be the three biggest developments in cybersecurity over the next 12-18 months?



If you indicated that you believe that cybersecurity should become more neurodiverse, why do you believe this to be the case?



SKILLS DIVERSITY

Dealing with the deficit

Ignoring the skills deficit will have a detrimental impact on cybersecurity in businesses

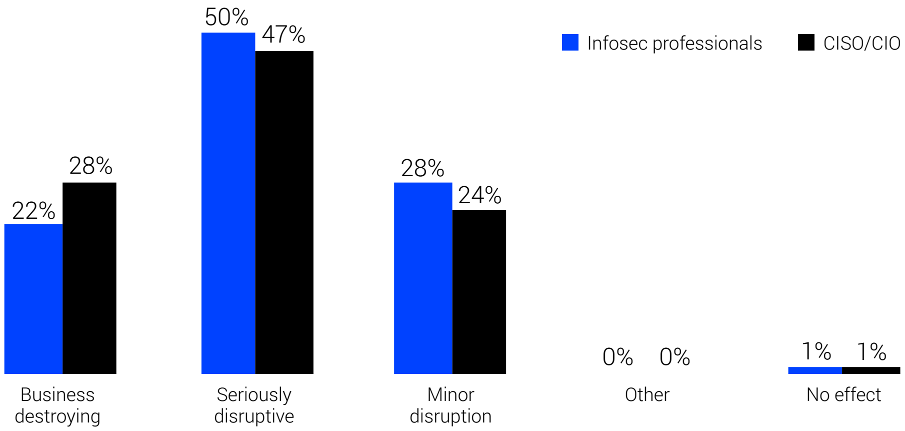
28% of CISOs and CIOs, and 22% of infosec professionals believe that if the skills deficit continues for another five years, that it will destroy businesses. And another half (50%) of infosec professionals believe that the skills gap will be seriously disruptive if it continues for the next 5 years.

28%
CISOs and CIOs

22%
infosec professionals

50%
believe that the skills gap will be seriously disruptive

What do you believe the effects will be on the industry as a whole if the skills deficit continues for another 5 years?



This differed considerably across Europe with only 11% of infosecs in Spain believing that if the skills deficit continues for another five years, that it will destroy businesses, compared to 29% in Sweden and 26% in the US.

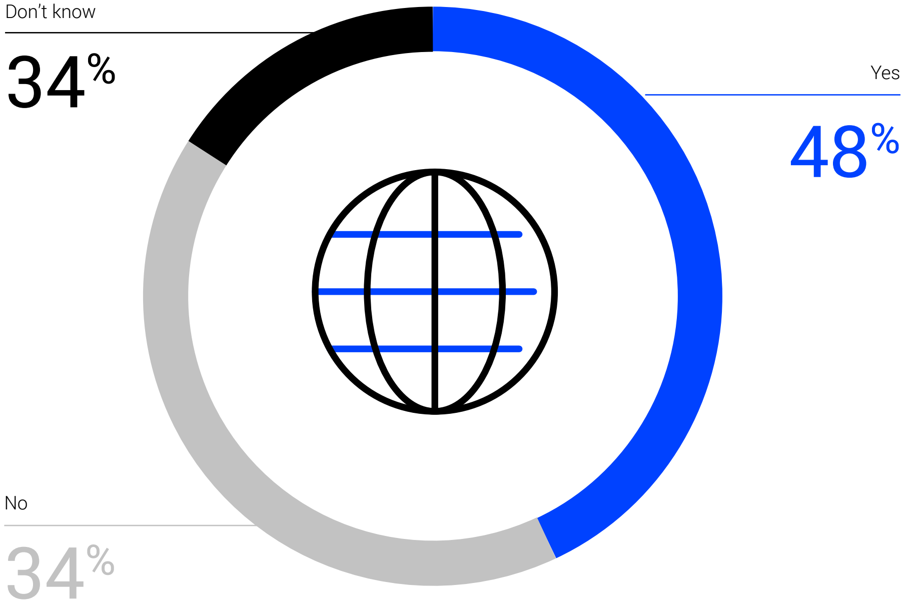
SKILLS DIVERSITY

Is the skills deficit everyone's problem?

Some companies in Europe aren't experiencing a skills deficit

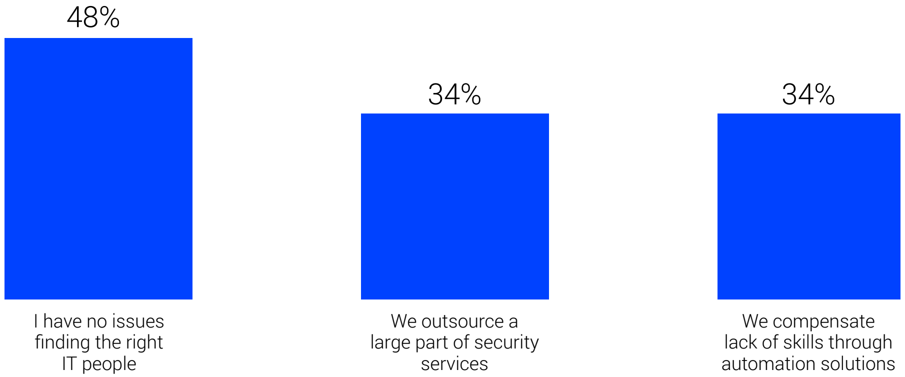
Despite CISO/CIOs and infosec professionals being concerned about the skills deficit, there is an almost equal split of companies who are negatively affected by the global cyber skills deficit (43%) and those who are not (41%).

Is your company negatively affected by the global cyber skills deficit?



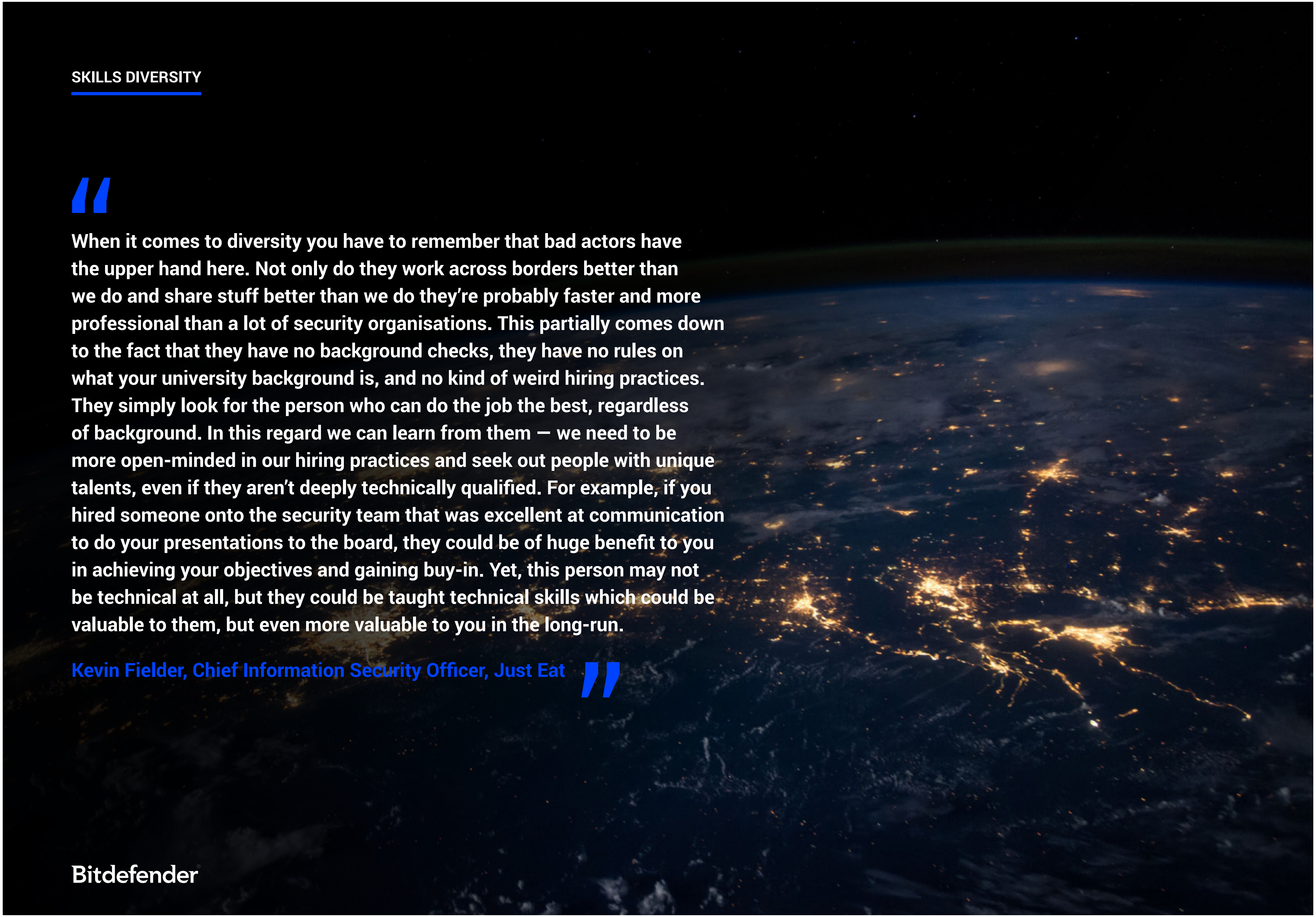
Of those that were not affected by the cyber skills deficit, just under half (48%) of infosec professionals believe it's because they have no issues with finding the right IT people. 34% believe that their company isn't affected by the cyber skills deficit because they compensate the lack of skills through automation.

Why is your company not affected by cyber skills deficit?



Compensaating for a lack of skills through automation is most popular in Australia/New Zealand and Germany (39%)

Over half (52%) of infosec professionals in the UK believe their company is not affected by the skills shortage because they have no issues finding the right IT people

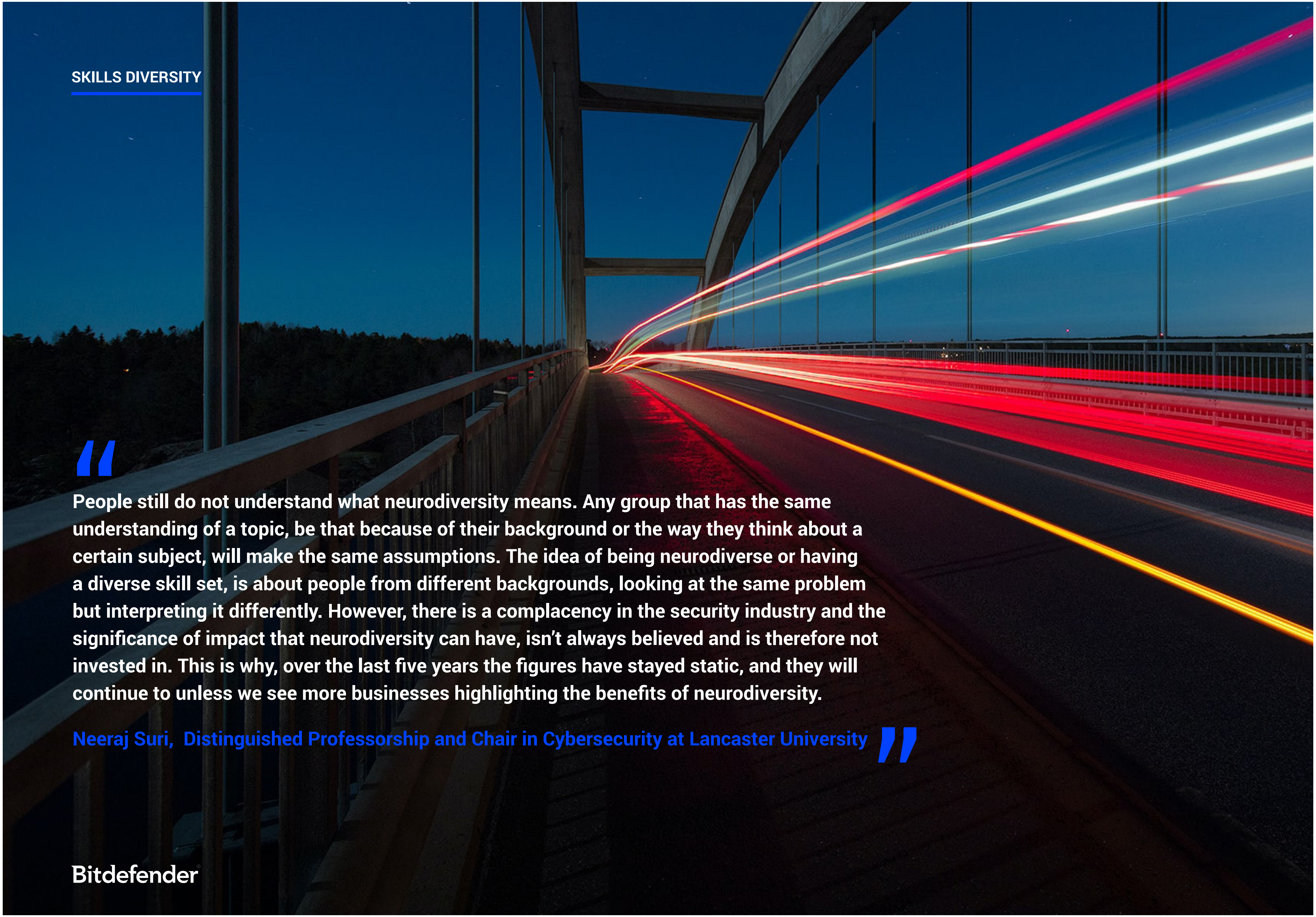


> “When it comes to diversity you have to remember that bad actors have the upper hand here. Not only do they work across borders better than we do and share stuff better than we do they’re probably faster and more professional than a lot of security organisations. This partially comes down to the fact that they have no background checks, they have no rules on what your university background is, and no kind of weird hiring practices. They simply look for the person who can do the job the best, regardless of background. In this regard we can learn from them — we need to be more open-minded in our hiring practices and seek out people with unique talents, even if they aren’t deeply technically qualified. For example, if you hired someone onto the security team that was excellent at communication to do your presentations to the board, they could be of huge benefit to you in achieving your objectives and gaining buy-in. Yet, this person may not be technical at all, but they could be taught technical skills which could be valuable to them, but even more valuable to you in the long-run.
>
> Kevin Fielder, Chief Information Security Officer, Just Eat”

“

There’s a famous quote from Leila Janah who said, “Talent is equally distributed but opportunity, is not“ and that is true in cybersecurity. Being successful in cybersecurity will come down to diverse representation. We have to focus on building teams that are not just balanced between men and women but that also include representative members from minority communities. We have to draw in people from different social groups, different ethnicities, different backgrounds and neurodiverse people. Not only will this ensure that we have a bigger talent pool to pull from to tackle the ever-present cybersecurity skills gap, but we’ll be enriched in diverse thinking power. And it’s this diverse thinking power that will ensure organisations are secured at every level.

Dr Jessica Barker, Socio-Technical Lead at Cygenta, Chair of ClubCISO ”



> People still do not understand what neurodiversity means. Any group that has the same understanding of a topic, be that because of their background or the way they think about a certain subject, will make the same assumptions. The idea of being neurodiverse or having a diverse skill set, is about people from different backgrounds, looking at the same problem but interpreting it differently. However, there is a complacency in the security industry and the significance of impact that neurodiversity can have, isn't always believed and is therefore not invested in. This is why, over the last five years the figures have stayed static, and they will continue to unless we see more businesses highlighting the benefits of neurodiversity.

Neeraj Suri, Distinguished Professorship and Chair in Cybersecurity at Lancaster University

RISE AND FALL (AND RISE AGAIN) OF RANSOMWARE

Why has ransomware fluxed in popularity, and is it here to stay? Infosec professionals explore how ransomware has changed over the last few years and whether companies know how to deal with it.

Bitdefender

RISE AND FALL (AND RISE AGAIN) OF RANSOMWARE

Ransomware is here to stay

The resurgence of ransomware is a huge concern for infosec professionals and recent events have only made it easier for cybercriminals

43% of infosec professionals agree that they are seeing a resurgence in ransomware attacks, but protection against them hasn't advanced much over the last five years. Just under half (49%) also stated that with increasing numbers of people working from home, their main cybersecurity concern is the business suffering a large-scale ransomware attack.

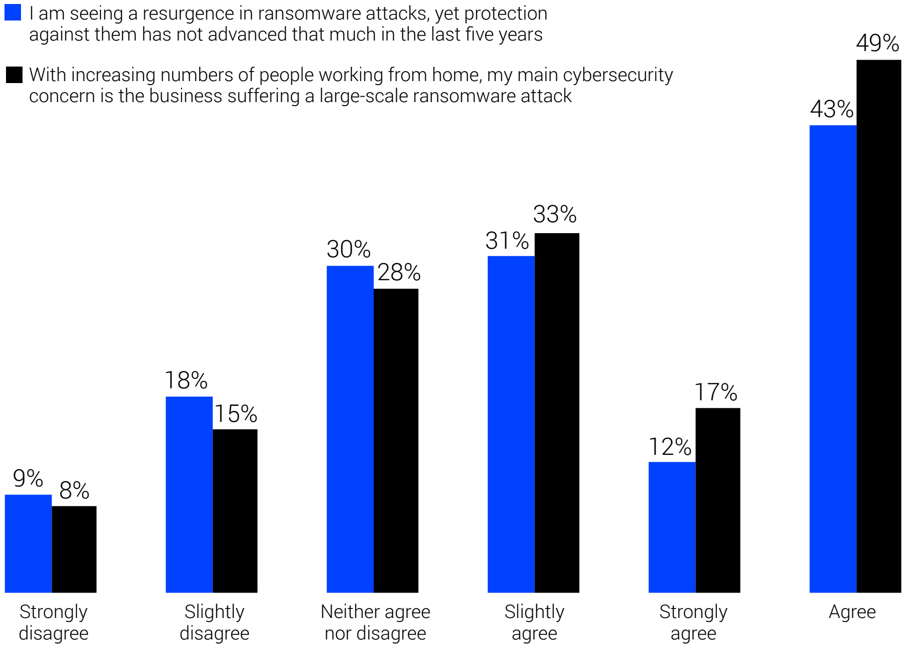
43%

seeing a resurgence in ransomware attacks

49%

concern is suffering a large-scale attack

Please indicate to what degree you agree or disagree with the following statements:



SKILLS DIVERSITY

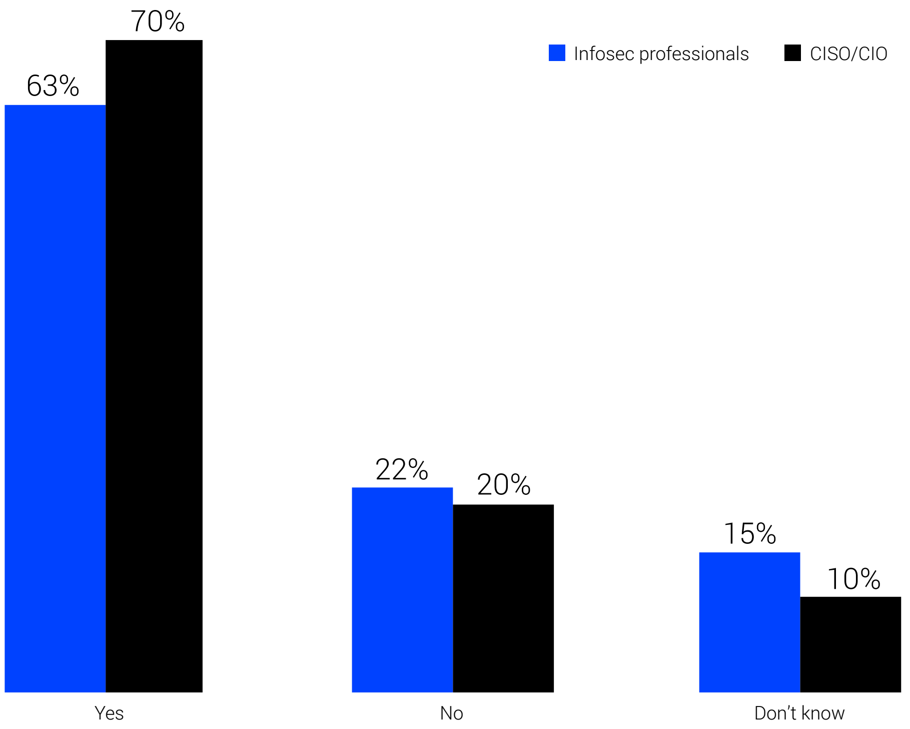
It could get even worse

Most infosec professionals believe that ransomware is due to get worse, but the jury is out

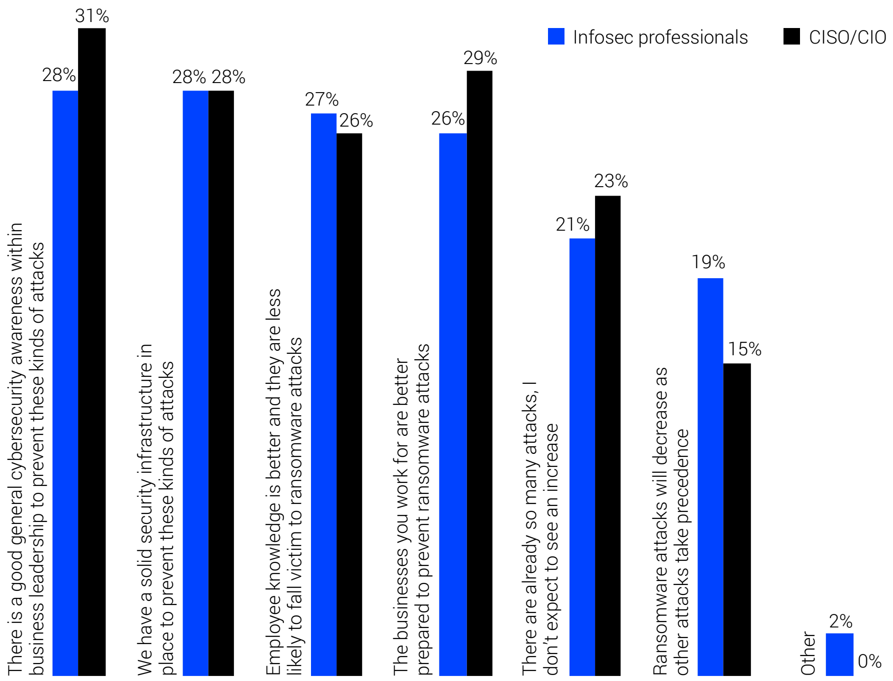
70% of CISOs/CIOs expect to see an increase in ransomware attacks in the next 12-18 months. This is a sentiment that is reiterated by 63% of infosec professionals.

Of those who don't think, or don't know, whether ransomware attacks will increase in the next 12-18 months, nearly 3 in 5 say it's because they have solid security infrastructure and there is good general cybersecurity awareness (28%).

Do you expect to see an increase in ransomware attacks in the next 12-18 months?



Why do you think that will be the case?



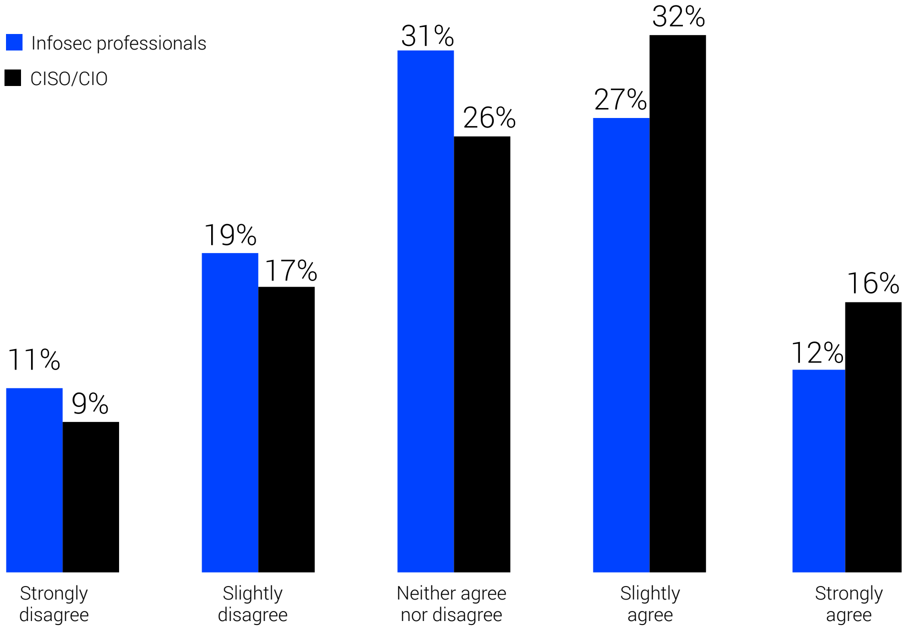
SKILLS DIVERSITY

Living with the consequences

Falling victim to ransomware has a significant impact on business

Almost half of CISOs/CIOs (49%) and just over two fifths of infosec professionals (42%) are worried that a ransomware attack could wipe out the business in the next 12-18 months if they don't increase investment in security.

Please indicate to what degree you agree or disagree with the following statements: "I am worried that a ransomware attack could wipe out the business in the next 12-18 months if we don't increase investment in security."



Nearly 2 in 5 infosec professionals reveal that the main consequences of a ransomware attack would be reputational damage (38%), increased downtime and disruptions to business continuity (36%). Legal fines and penalties were of least concern, with only 27% citing as the the main consequences of a company suffering a ransomware attack.

What would be the main consequences of your company suffering a ransomware attack? Select all that apply

38%
Reputational damage

36%
Increased downtime and business continuity disruptions

35%
The personal impact on people (customers, staff, vendors)

33%
Loss of revenue

30%
Increased cost of cyber insurance

29%
Paying to have the ransomware deactivated

27%
Legal fines and penalties

0%
Other

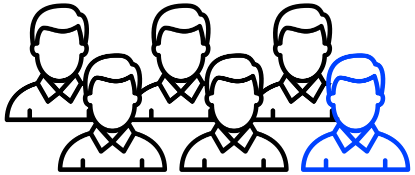
3%
Don't know

RISE AND FALL (AND RISE AGAIN) OF RANSOMWARE

Paying up

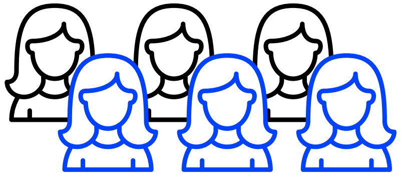
A surprising amount of infosec professionals believe their organisation would pay up should they be attacked with ransomware

Almost one in six CISOs/CIOs (59%) and half of infosec professionals (50%) believe that the business they work for would pay the ransom in order to prevent its data/information from being published. And a further 18% of infosec professionals, don't know whether the business they work for would pay the ransom.



1 in 6

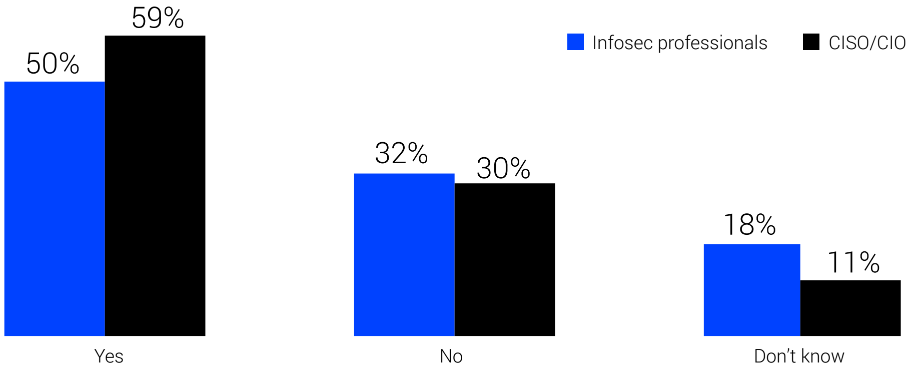
CISOs and CIOs believe that the business they work for would pay the ransom



50%

infosec professionals believe that the business they work for would pay the ransom

Should the business you work for suffer a ransomware attack, do you believe it would pay their ransomware in order to prevent its data/information from being published?



Those in the UK and Denmark are most likely to expect their organisation to pay a ransomware order (both 56%)

INCREASED USE OF IoT BUT NO KNOWLEDGE OF PROTECTION

The use of IoT devices is on the rise, but there is a clear disparity between the increased use of connected devices and the lack of security being implemented. This is leaving both businesses and consumers open to an array of potential threats.

Bitdefender

INCREASED USE OF IOT BUT NO KNOWLEDGE ON PROTECTION

IoT devices are easy to hack

Infosec professionals are concerned about the vulnerabilities of IoT devices

45% of CISOs/CIOs and 2 in 5 infosec professionals (40%) believe that it's easy for hackers to gain control of the IoT devices which are being used by employees from home for business purposes. Respondents from Germany and Italy have the least confidence with regards to their security of IoT devices from hackers while employees work from home (16% and 20%).

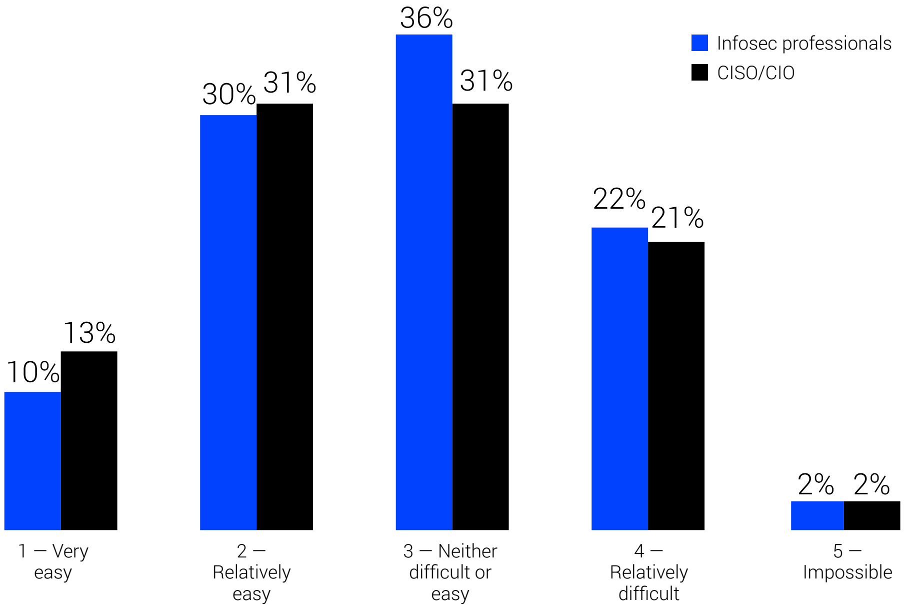
16%

Germany

20%

Italy

On a scale from 1 to 5, with 1 being very easy and 5 being impossible, how easy do you think it is for hackers to gain control of the IoT devices being used for business purposes, by employees working from home in general?



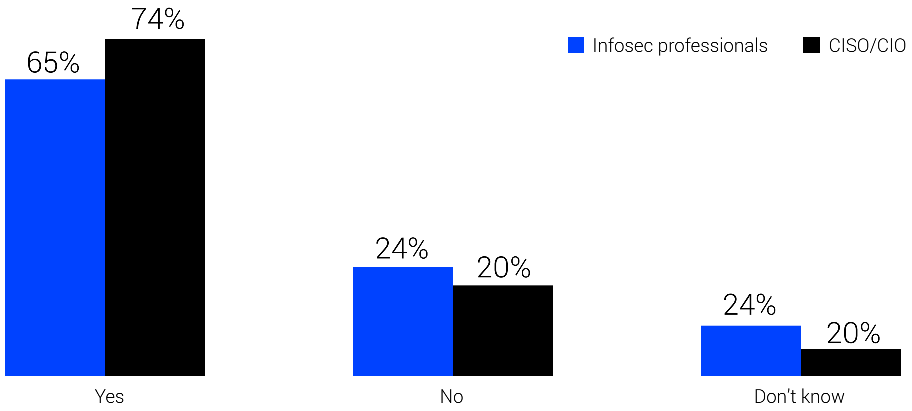
INCREASED USE OF IOT BUT NO KNOWLEDGE ON PROTECTION

Keeping up with IoT

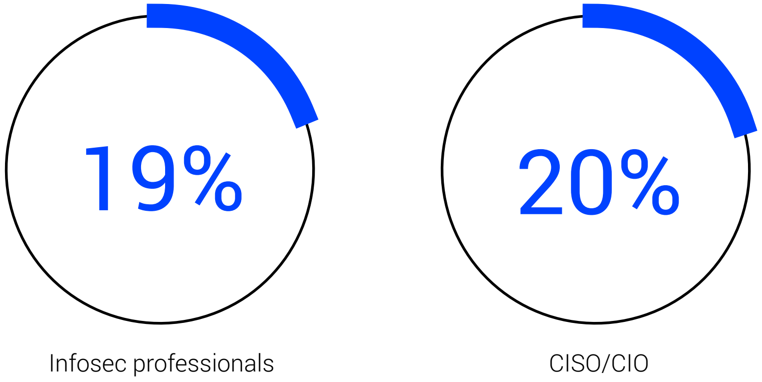
While knowledge on how to keep IoT devices safe is getting better, cybersecurity is struggling to keep up

Nearly two thirds of infosec professionals (65%) believe that, as a result of the increased use of IoT devices, the security knowledge on how to protect these devices has improved within their business. Confidence on this matter rises to 74% amongst CISOs/CIOs.

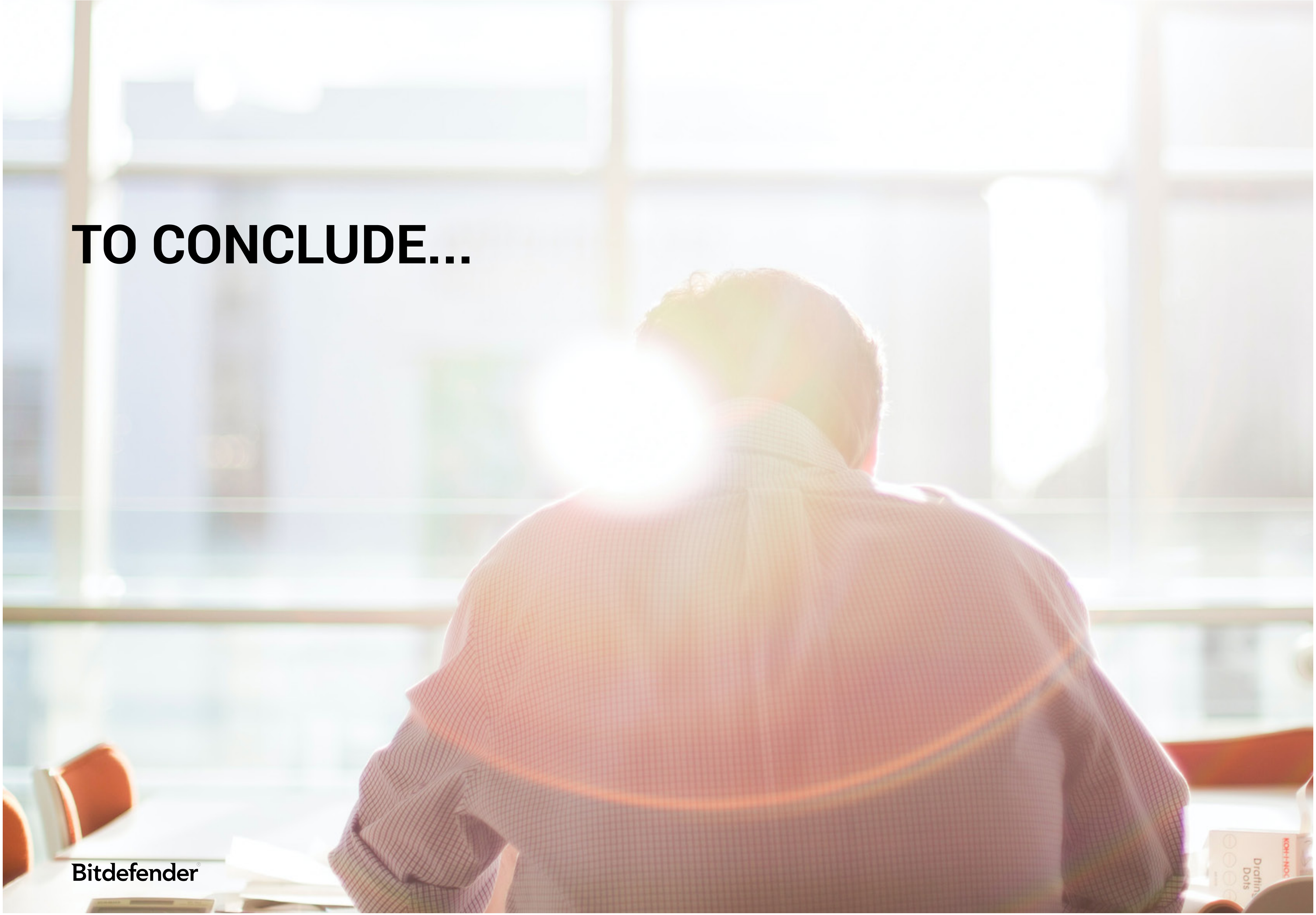
As the use of IoT devices in business increases, do you think the security knowledge on how to protect these devices in your business has also improved?



In your opinion, what will be the three biggest developments in cybersecurity over the next 12-18 months?



However, nearly a fifth of infosec professionals (19%) and a fifth of CISOs/CIOs say, in relation to the three biggest developments in cybersecurity over the next 12-18 months, that IoT devices will continue to spread faster than they can be secured.



TO CONCLUDE...

Bitdefender

CONCLUSION

“

It’s time to move away from a culture of risk aversion, checklists and specific systems. The consequences of viewing cybersecurity as a checklist activity opens the door to threats which can be easily avoided by taking a more holistic approach cybersecurity. Infosec leaders and professionals need to take a step back and ensure that teams working on security are neurodiverse and have the necessary skills. They also have to make sure that the wider business understands the importance of security. This is especially relevant in the COVID-19 era where working from home makes businesses more susceptible to attacks.”

“Over half of infosec professionals agreed that the way cyber security is communicated in their business needs to change if they are to increase investment. Improved sharing between infosec professionals is one way to achieve this.”

“The threat of cyberwarfare goes beyond what is seen in the media. While places such as hospitals and power stations are obvious targets, so too are other businesses, and the threat shouldn’t taken lightly. This is why it is so important for businesses to invest in cyber security defences. Those that ignore it are opening themselves up to severe consequences, ones that could be detrimental to the longevity of the business.”

“Ransomware has proved it is here to stay. As much as it may have dipped a few years ago, it has resurged with a vengeance. Many infosec professionals are rightfully concerned about their companies suffering ransomware attacks and expect them to increase within the next year. Yet, many of these professionals doubt that their business would follow the standard guidelines and would pay the ransom in order to protect their companies data and reputation. This is likely why ransomware continues to prevail. Only when they stop giving in to such demands will we see the long term demise of ransomware. ”

Liviu Arsene, Global Cybersecurity Researcher, at Bitdefender

CONCLUSION

“Despite the very real concerns the lack of diversity, and neurodiversity, has on the industry, it’s interesting to see that there has been very little improvement over the last five years. Investing in neurodiversity will be especially important if the industry, and cybersecurity professionals defending the enterprise, want to stand their ground and triumph over bad actors. By investing in diversity, and the right skill sets, organisations and the industry will be future proofing themselves itself from the inside out.”

“It’s not uncommon for a household to have some sort or voice assistant or a connected device in their home these days, but many rarely spare a thought for how to protect it. With the increase in people working from home looking set to continue long term and people increasingly using IoT devices for work related matters, it opens doors for cybercriminals. Not just into employee’s homes, but also potentially into their workplaces. The issue with IoT devices is that they are advancing at such a rate security simply can’t keep up. This is why IoT security has to be front of mind for Infosec professionals.”

“Overall, the cybersecurity industry is facing some unique challenges as newer technologies come on the scene. At the same time, it is struggling with older issues. Ultimately in order to fully address some of the previous issues such as ransomware and neurodiversity, the cybersecurity industry has to learn to better communicate. This doesn’t just apply in terms of how we communicate with each other, but also how we talk about the threats outwardly. Whether it is securing businesses against cyberwarfare or encouraging more diverse talent into the industry, we have to start breaking down barriers or the impact will be detrimental. Not just to businesses, but potentially whole economies. ”

Bogdan Botezatu, Director or Threat Research at Bitdefender

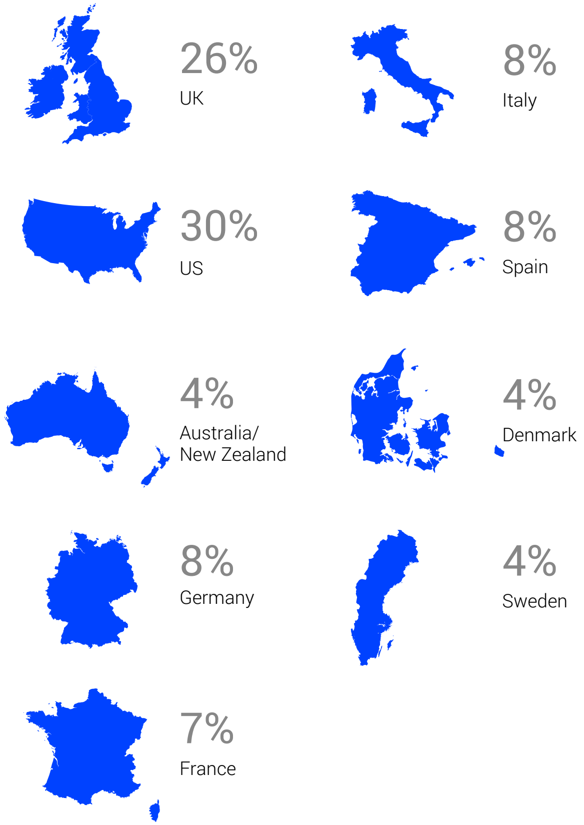
SURVEY METHODOLOGY

Survey Methodology

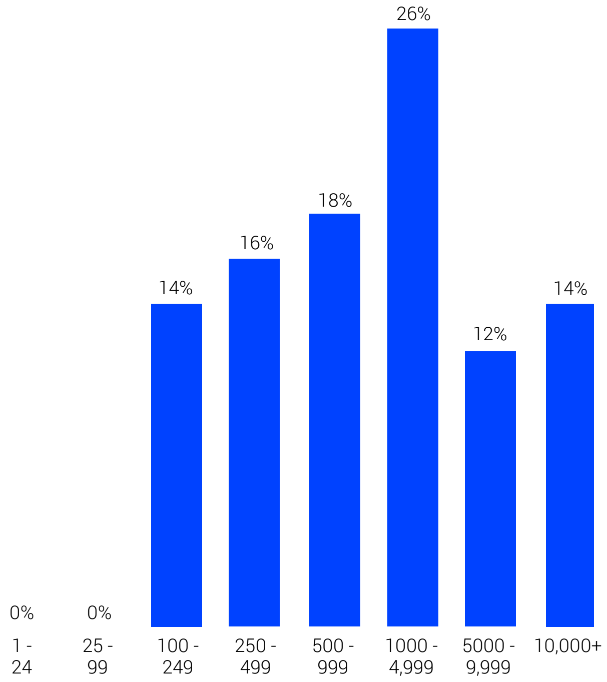
The 10 in 10 survey was conducted among 6724 respondents with a job role in or decision-making influence over cyber security in companies with 100 or more employees.

The interviews were conducted online by Sapio Research in May 2020 using an email invitation and an online survey.

Respondents by geography



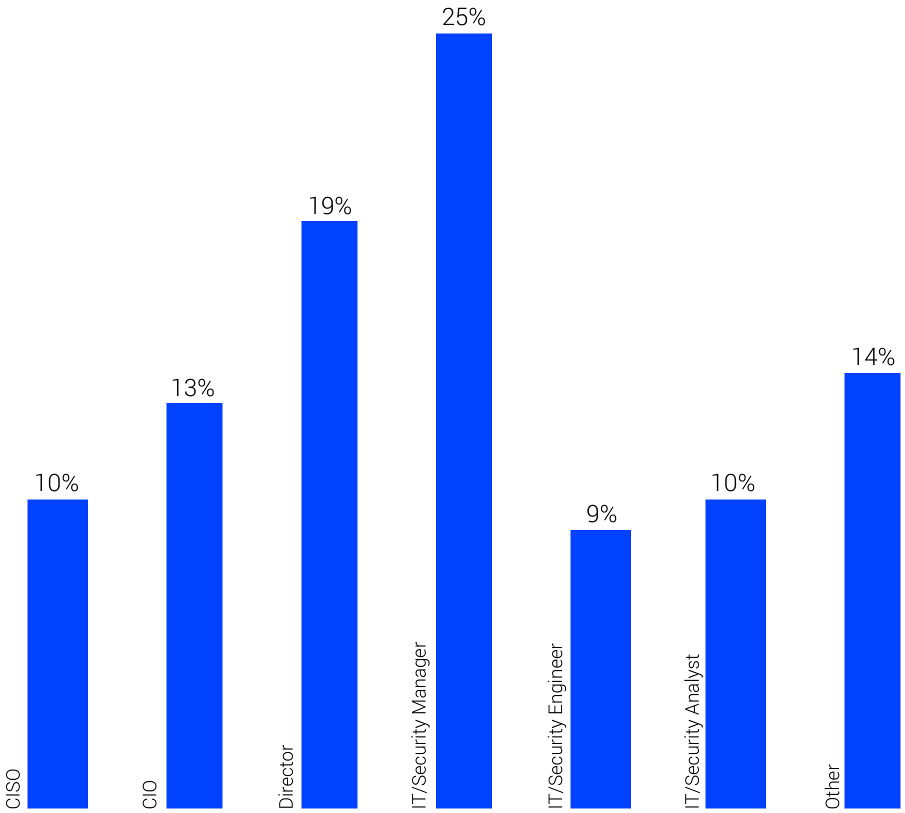
Respondents by number of employees



SURVEY METHODOLOGY

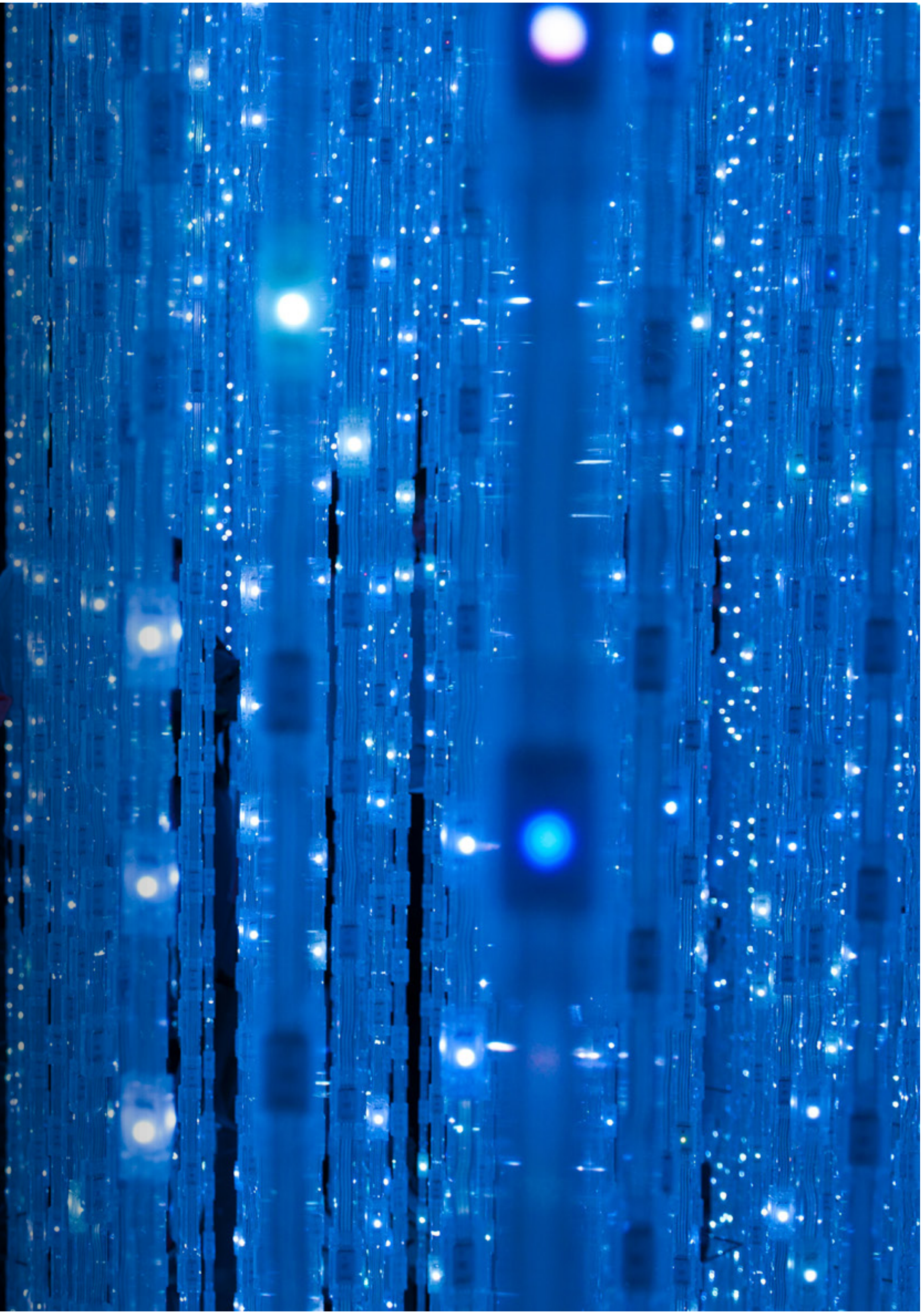
Survey Methodology

Respondents by job title



Respondents by industry sector

13%	Technology	3%	Professional Services (Accounting, Legal, Management, Marketing/Advertising)	1%	Media & Entertainment
10%	Finance	3%	Transportation	1%	Agriculture
8%	Healthcare	3%	Biotech	1%	Utility
7%	Government	2%	Legal	1%	Shipping
6%	Education	2%	Chemical	1%	Not-for-Profit/ Third sector
6%	Manufacturing/ Automotive	2%	Food & Beverage	1%	Pharmaceuticals
5%	Retail	2%	Telecom	6%	Other
5%	Construction	2%	Energy		
4%	Electronics	2%	Hospitality		
4%	Insurance	1%	Apparel		



About Bitdefender

Bitdefender is a global security technology company that provides cutting edge end-to-end cybersecurity solutions and advanced threat protection to more than 500 million users in more than 150 countries. Since 2001, Bitdefender has consistently produced award-winning business and consumer security technology and is a provider of choice in both hybrid infrastructure security and endpoint protection. Through R&D, alliances and partnerships, Bitdefender is trusted to be ahead and deliver robust security you can rely on.

Contact Us

🌐 **www.bitdefender.com**

☎ **Andrei Taflan: +4 0731 496 792**

☎ **Mihaela Filip +40 728 600 190**

@ **publicrelations@bitdefender.com**

🐦 **twitter.com/Bitdefender_Ent**

Bitdefender®