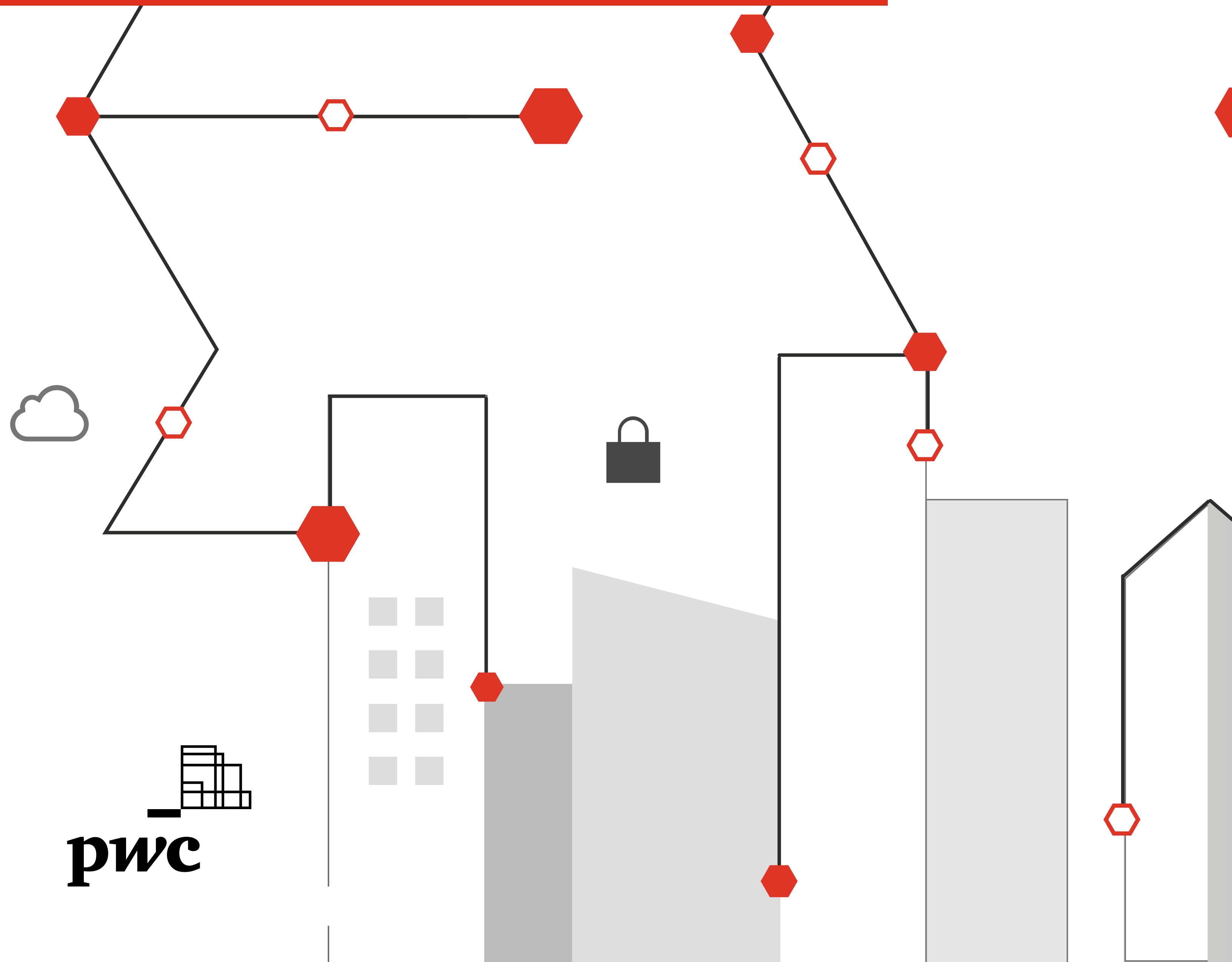
Global Digital Trust Insights Survey 2021

The Netherlands

Cybersecurity comes of age



Content

Cybersecurity comes of age

Five moves to get to the next level

Just decades after coming out from under IT's wing, the cybersecurity profession has matured. Since the Massachusetts Institute of Technology was granted the first US patent for a cryptographic communication system in 1983, the industry has grown by leaps and bounds — with a long list of growing pains.

Armed with the insight and foresight that only experience and wisdom can provide, cyber stands at a critical, pivotal and exciting time for the industry and the organizations and people it serves. Our findings from the Global Digital Trust Insights 2021 survey of 3,249 business and technology executives around the world, including 54 in the Netherlands tell us what's changing and what's next in cybersecurity.

No longer solely reactive — although it is that — cybersecurity has become more thoughtful and forward-thinking, with the knowledge and technologies to stop attacks before they start.

No longer technology-focused — although tech is very much in the picture — security leaders are working closely with business teams to strengthen and increase the resilience of the organization as a whole. As a result, cyber is leveling the playing field with attackers, pushing back and fending off as never before.

The timing couldn't be better. Recent shifts in business models have prompted many enterprises to speed up their digitization programs, although we see in the Netherlands that the pace is a bit behind. CEOs and boards are turning to their CISOs for help increasing their resilience and creating business value.

Technology is maturing, too, simplifying cybersecurity's work and integrating it with the business as a whole. Digital solutions are adding layers of protection and continuously monitoring systems automatically for a simpler, more integrated approach to security.

1 Reset your cyber strategy, evolve leadership for these new times

Business transformations are more sweeping and rapid, but less so in the Netherlands

In the pandemic's first three months, CEOs report, their organizations digitized at surprising speed, advancing to year two or three of their five-year plans. The future is now: digital health, industrial automation and robotics, enhanced ecommerce, customer service chat bots, virtual reality-based entertainment, cloud kitchens, fintech, and more have arrived.

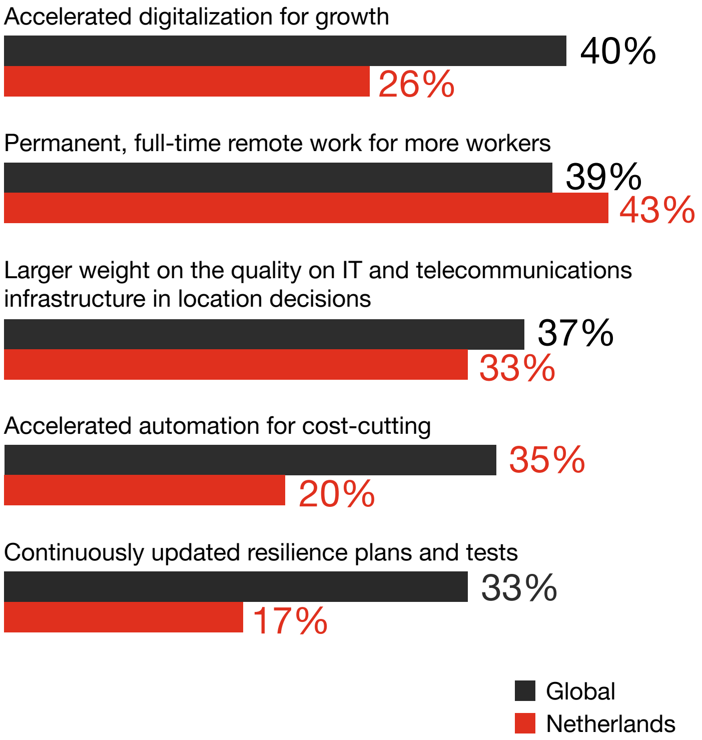
The health crisis and economic recession have stoked further change globally, but not as much in the Netherlands. According to our Global DTI 2021 survey: 40% of executives say they're accelerating digitization, in the Netherlands, only 26% say the same.

Their digital ambitions have skyrocketed. Twenty-one percent are changing their core business model and redefining their organizations (the "redefiners"), while 18% are breaking into new markets or industries (the "explorers"). Both categories have doubled since our survey last year.

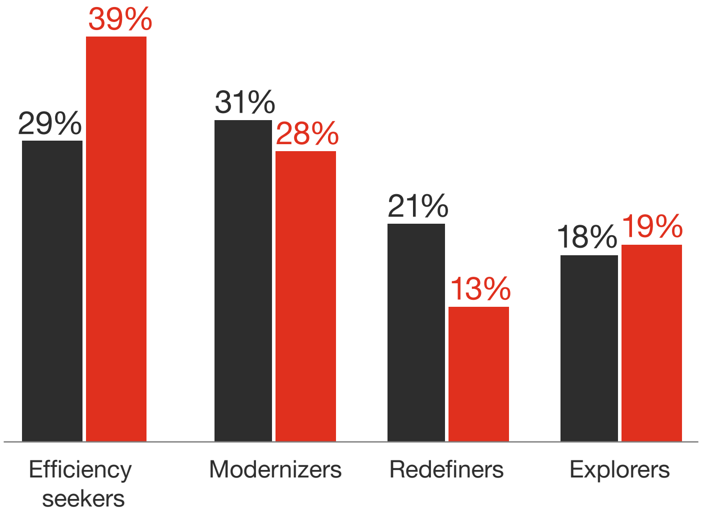
Doing things faster and more efficiently is the top digital ambition for 29% of executives ("efficiency seekers"), while 31% are modernizing with new capabilities ("modernizers"). More than one-third — 35% — say they're speeding up automation to cut costs, which is no surprise at a time when revenues are down.

In the Netherlands however, fewer respondents (13%) are looking to change their core business model, while more executives (36%) want to keep doing what's always been done, only more efficiently - implying that the effects are relatively less drastic here.

Businesses are changing...



...and their ambitions are rising...



Source: PwC Global Trust Insights Survey 2021, October 2020: base 3,249
Q: What is the primary aspiration for your enterprise-wide, technology-driven business transformation or major digital initiatives?

New times call for a resetting of cyber strategy

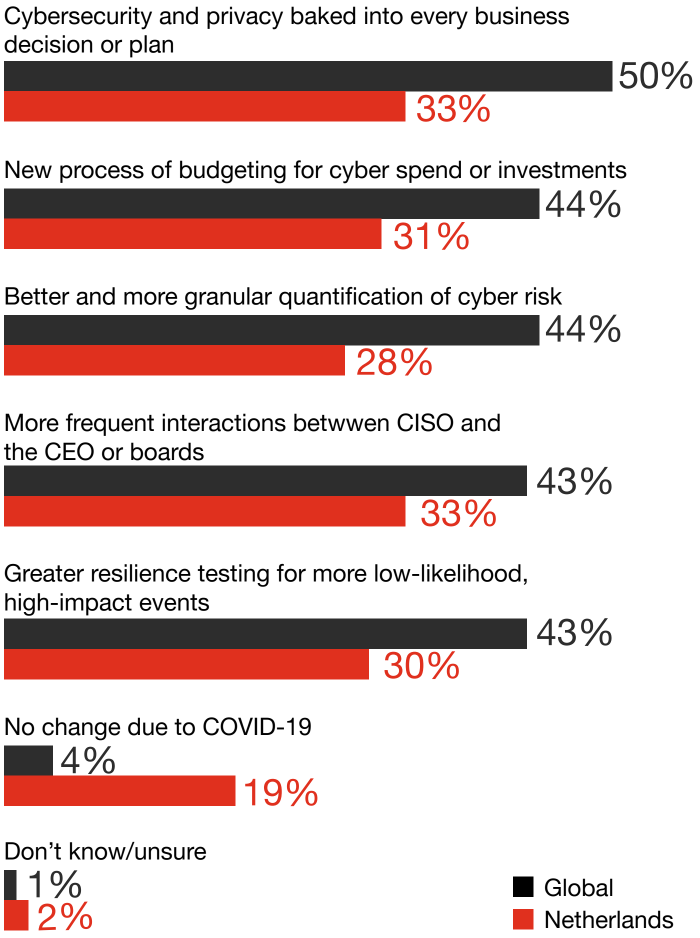
New technologies and business models — and the fast pace of adoption — bring new risks and a different way to determine cyber strategies.

Savvy CISOs are in step with the vision and goals of their enterprise as a whole, and the environment in which it resides. “Cybersecurity is a growing problem of the entire society and requires all of us to reinvent ourselves and help society. It is not about just basic internal hygiene or good housekeeping, but also in every engagement and aspect of our life” said Aernout Reijmer, CISO, ASML.

Nearly all (96%) respondents say they’ll shift their cybersecurity strategy due to COVID-19, but in the Netherlands only 81% will be making any changes. Half are more likely now to consider cybersecurity in every business decision — that’s up from 25% in our survey last year, but only a third in the Netherlands are likely to do the same.

Improved ways in identification and quantification of cyber risk is important for 44% of the respondents, less so for The Netherlands with 28% of the respondents.

...and so are their cyber strategies



Source: PwC Global Trust Insights Survey 2021, October 2020: base 3,249

“

Cybersecurity is a growing problem of the entire society and requires all of us to reinvent ourselves and help society. It is not about just basic internal hygiene or good housekeeping, but also in every engagement and aspect of our life.

—Aernout Reijmer
CISO, ASML

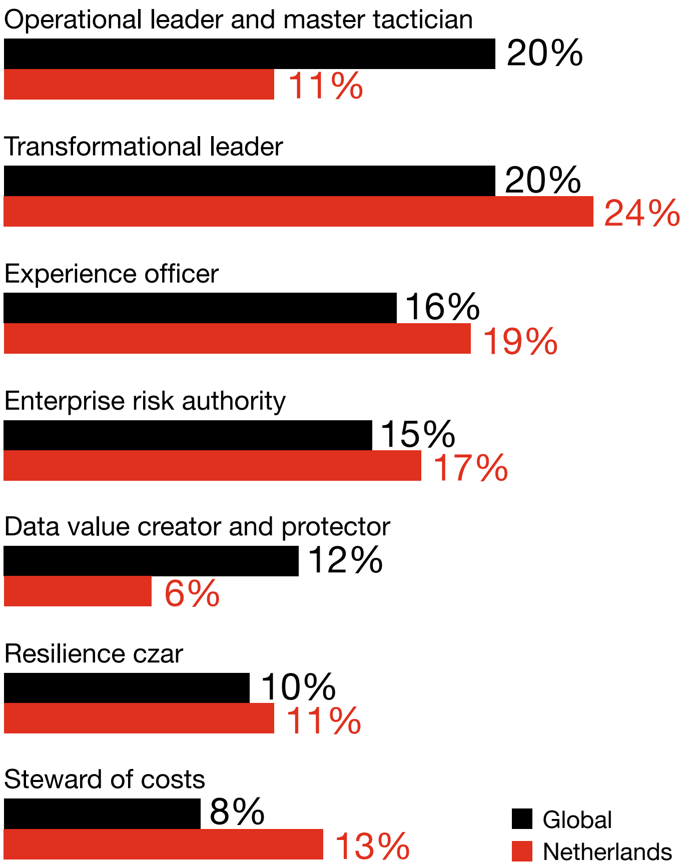
CISOs are evolving to the needs of business

New times also call for new CISO leadership modes. The top two leadership modes chosen by executives for a CISO were a “transformational leader” (20%), and an “operational leader and master tactician” (20%), whereby the Netherlands’ focus is on “transformational leader” (24%) and “experience officer” (19%).

These roles are encompassing and call for the multifaceted expertise and experience that CISOs have built up. The transformational CISO leads cross-functional teams to match the speed and boldness of digital transformations with agile, forward-thinking security and privacy strategies, investments, and plans. The operational leader and master tactician is a tech-savvy and business-savvy CISO who can deliver consistent system performance, with security and privacy throughout the organization and its ecosystem amid constant and changing threats.

Some CISOs already inhabit these roles, and are exhibiting the three qualities most prized by executives: strategic thinking (38%), the ability to take smart risks (38%), and leadership skills (36%).

CISOs need to play encompassing roles to help



Source: PwC Global Trust Insights Survey 2021, October 2020: Base 3,249
Q: What is the primary role your organization’s CISO needs to play to help your organization achieve its growth and strategic objectives in the next two years?

From cybersecurity to digital trust

It’s a critical juncture for cybersecurity and CISOs. A business-driven cyber strategy is the single most important step for business and security leaders amid sweeping, rapid business digitization. This reset not only defines the expanding role of the CISO, it also affects the way the organization sets cyber budgets, invests in security solutions, plans for resilience, and enhances its security organization. It determines whether CISOs may grow to become stewards of digital trust, able to lead their organizations securely into the new era with strategies to protect business value and to create it.

2 Rethink your cyber budget to get more out of it

Cyber budgets will rise for half of the businesses surveyed

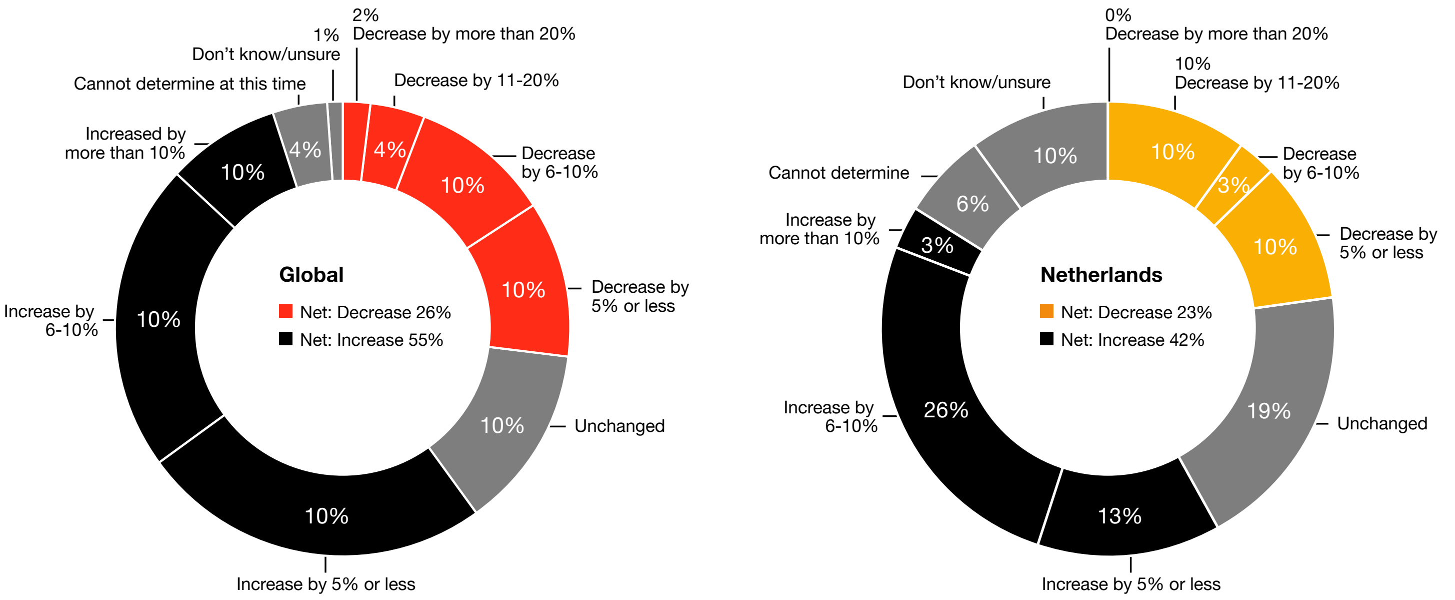
Fifty-five percent of technology and security executives in our Global DTI 2021 survey plan to increase their cybersecurity budgets, with 51% adding full-time cyber staff next year — even as most (64%) executives expect business revenues to decline in 2021. Clearly, cybersecurity is more business-critical than ever before.

Still, 26% will need to do more with less, and 13% will have to make do with static budgets.

“The circumstances we find ourselves in with the economy are putting a lot of pressure on security organizations to make sure that the investments we’re making are efficient and cost-effective,” says Katie Jenkins, CISO, Liberty Mutual.

Getting the most value for every cybersecurity euro spent becomes more critical as entities digitize: every new digital process and asset becomes a new vulnerability for cyber attack.

More are increasing cyber budgets than decreasing them in 2021



Source: PwC, Global Digital Trust Insights Survey 2021, October 2020: base 3,249
Q: How is your cyber budget changing in 2021? base 1,414

Most lack confidence in the budgeting process

More than half (65%) of business and tech/security executives in the Netherlands lack confidence that cyber spending addresses the most significant risks. Or that their budget funds remediation, risk mitigation and/or response techniques that will provide the best ROI (67%). Or that budgets provide the resources needed for a severe cyber event (72%). Or that the process monitors the cyber program's effectiveness compared to expenditures (78%).

Cyber budgets could — and should — link to overall enterprise or business unit budgets in a strategic, risk-aligned, and data-driven way, but 63% in the Netherlands lack confidence that their current process does this.

And with regard to preparedness for future risks, they are not confident that cyber budgets provide adequate controls over emerging technologies (69%).

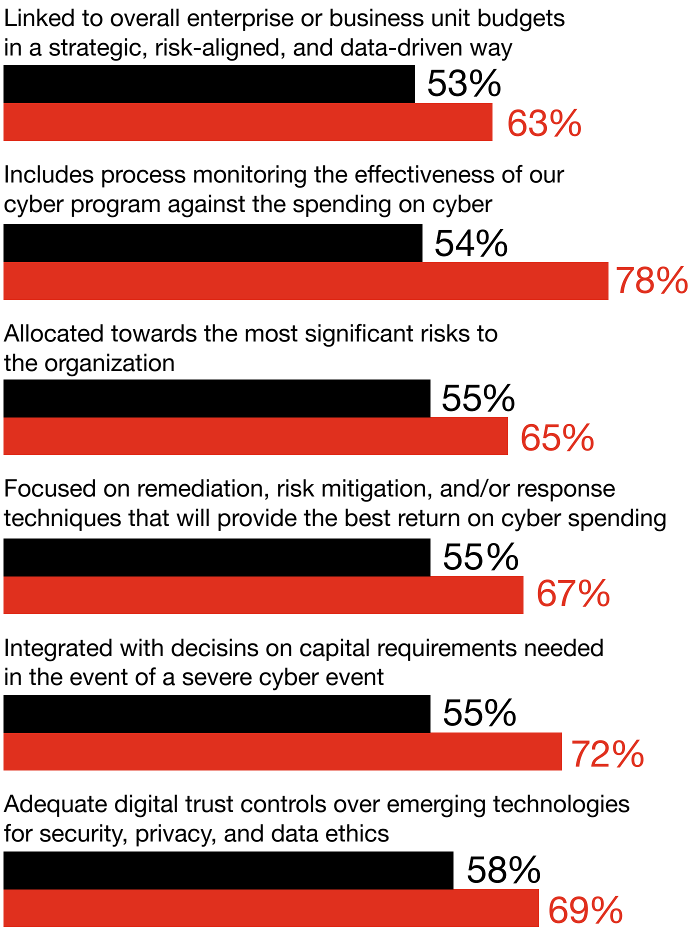
With confidence lagging in the process used to fund cybersecurity, this indicates that it's time for an overhaul. However, only 31% of respondents in The Netherlands will be trying new budgeting processes (compared to 44% globally).

Companies should investigate how cyber security can enable the deployment of emerging technologies securely into this fast changing digital world, otherwise cyber security will hinder business agility in the end. Furthermore, it is important to ensure that we invest wisely and focus cyber budgets on those areas which will have the most impact on reducing the overall risk profile.

Confidence in current cyberbudgets and processes is low today

(Percentage of respondents who are not 'very confident')

Our cyber budget/process is:



Source: PwC, Global Digital Trust Insights Survey 2021, October 2020: base 3,249
Q: Regarding your organization's current cyber budget and processes, how confident are you with regard to the following?

Putting a euro amount on cyber risk is a must

Cyber managers can do more with less, but to do so they need to put a euro amount on cyber risk and use the information to make smart choices that protect the business's security, privacy, *and* cash flow.

Seventeen percent of the executives in our Global DTI survey have quantified cyber risks, and are realizing benefits from doing so. A highly acquisitive company that quantifies cyber risks can evaluate deal opportunities faster and more systematically. A financial institution that handles millions of transactions a day can do daily and weekly threat and vulnerability assessments — staying alert to the performance of underlying controls and any need to reallocate resources.

Cyber risk quantification is not for the faint-hearted, with many obstacles in the way: lack of a standard model, lack of people who understand cyber and risks from a business lens, and lack of scalability. Nevertheless, nearly 60% are beginning to quantify risks or have implemented at scale. And nearly everyone else (17%) plans to begin risk quantification within the next two years.

We observed that respondents in the Netherlands seem to be slightly behind compared to the global aggregate regarding initiatives required for improved cyber risk management (including better quantification of cyber risks). A smaller proportion of companies in the Netherlands are realising benefits from these initiatives, but more companies plan to do them in the nearest future.

Raising confidence in budget decisions

The economics of cybersecurity has long focused on the cost side (compliance, updating capabilities, and so on). This must change. The cyber strategy reset — considering cybersecurity in every business decision — means connecting cyber budgets to overall enterprise or business unit budgets in a strategic, risk-aligned, and data-driven way.

Putting a euro amount on the value of a cyber project, in terms of risk reduction or less costly compliance, allows comparison of the costs and value of cyber investments so they can be prioritized. Quantification also makes it easier to measure the value of the overall portfolio of cyber investments against business objectives. This kind of rigor and sophistication will be increasingly demanded — especially as the markets and regulators hold CEOs and board members more accountable for cybersecurity and privacy.

3 Invest in every advantage to level the playing field with attackers

New technologies turning the tables on cybercrime

Innovation is changing the cybersecurity game, giving new advantages to defenders and leveling the playing field with attackers. Cyber startups are hot: in the past decade, some two dozen have attained IPO or M&A values of $1 billion, 10 of them in the last two years, according to CB Insights.

And the existing array of cyber solutions has matured, enabling a shift to Zero Trust architectures, real-time threat intelligence, security orchestration and automation, advanced endpoint protection, identity and access management, and other advanced technologies — prompted in large part by a threefold growth in cloud services.

Early switchers have taken advantage of these developments. But, more important, they're investing in the classic digital transformation trifecta — *people, processes, and technologies* — to close the wide lead that attackers have long held.

In our Global DTI 2021 survey, we looked at 25 new cybersecurity approaches and practices (see chart) and tracked the measures on which organizations say they've made significant progress.

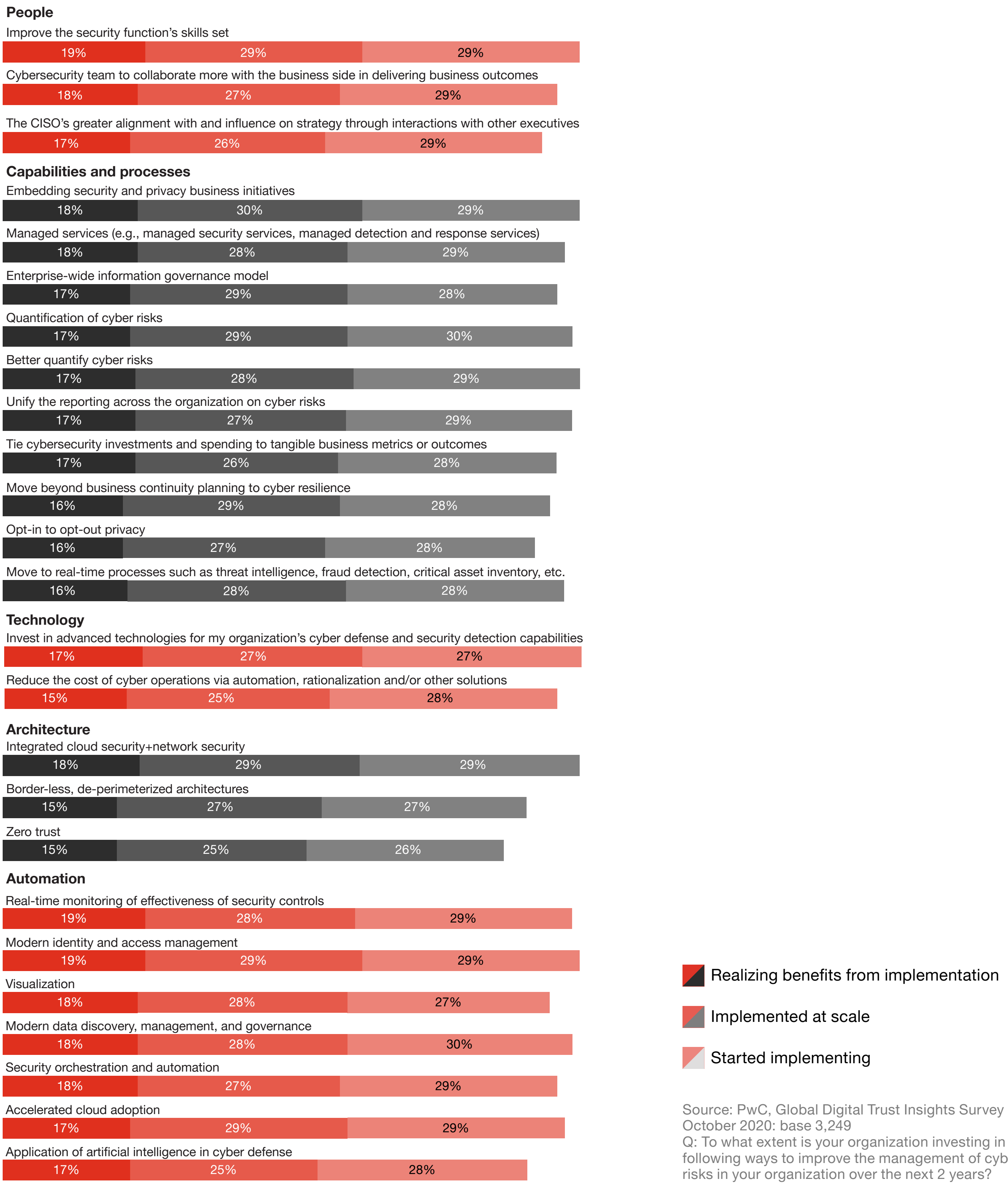
New approaches and mindsets of the early switchers

A minority — between 15% and 19% — of executives say they're already benefiting from some of these new practices. This is the group we call early switchers.

Executives from large organizations ($1B+) are more likely to report benefits from making a strategic shift (their "cybersecurity team collaborates more with the business side in delivering business outcomes"); switching to advanced technologies ("investing in advanced technologies to improve the effectiveness of my organization's cyber defense and security detection capabilities"); and restructuring operations ("reducing the cost of cyber operations via automation, rationalisation and/or other solutions.")

Executives from the largest organizations ($10B+) are more likely to report gains from using security models and technologies such as Zero Trust, managed services, virtualization, and accelerated cloud adoption.

Businesses are moving to new approaches and thinking to improve cybersecurity



Source: PwC, Global Digital Trust Insights Survey 2021, October 2020: base 3,249
Q: To what extent is your organization investing in the following ways to improve the management of cybersecurity risks in your organization over the next 2 years?

The greater the transformation, the higher the odds of significant progress

Overall, the 3,249 survey respondents reported making ‘significant progress’ over the past three years on an average of **six** measures, signaling better risk management, greater resilience, increased stakeholder trust, or faster implementation of digital transformation. The top outcomes — reported by 43% of executives — are improved customer experiences, quicker responses to incidents and disruptions, and better prevention of successful attacks.

But an elite group of early switchers — those who report realizing benefits across 20 or more of the 25 new practices — say they have made significant progress on at least **12** outcomes.

On the other hand, those who haven’t yet shifted to new practices tend to report significant progress on only two or three outcomes.

These findings suggest that investing in every advantage in technologies, processes and the capabilities of your people is critical to making meaningful headway against attackers. And it underscores the importance of CISOs who can serve as transformational leader or operational leader/master tactician.

“Collaboration is crucial. No one can or should face this challenge on its own. We built this world together, now we need to protect it together.” says Luisella ten Pierik, CISO at Stedin.

Progress on cybersecurity goals in the past three years (indexed scores)

Better risk management

Global	74%
Netherlands	66%

- Less burdensome employee experience
- Lower costs of compliance
- Lower costs of managing risks

Greater resilience

Global	77%
Netherlands	68%

- Faster response times to disruptions
- Lower downtime and associated costs
- Increased prevention of successful attacks

Greater trust

Global	76%
Netherlands	69%

- Higher customer loyalty
- Improved net promoter score
- Greater compliance with regulations
- Improved confidence of leaders

Business enablement

Global	76%
Netherlands	68%

- Accelerated entry into new markets
- Expedited launch of new products
- Improved customer experience
- Improved employee experience
- More successful transformations

Source: PwC, Global Digital Trust Insights Survey 2021, October 2020: base 3,249
Q: How much progress has your organization made in cybersecurity in the past three years?

> “Collaboration is crucial. No one can or should face this challenge on its own. We built this world together, now we need to protect it together.

—Luisella ten Pierik
CISO, Stedin

Cloud security is the next big switch

Companies are rapidly moving their operations (75%) and security (76%) to the cloud. They're doing away with static, inherently insecure legacy systems in favor of more dynamic, nimble integrated cloud/network systems that are secure by design.

CISOs who transition their organization to the cloud are able to build in hygiene mechanisms from the beginning — in automated ways. They're also able to eliminate friction from the system and simplify service delivery to their customers.

More than a third (35%) of executives strongly agree that moving to the cloud is foundational for the next generation of business solutions for their organization. And 36% strongly agree that new solutions exist to secure cloud infrastructures better than they have ever been in the past.

Small and medium-size organizations can also modernize

Larger organizations with more resources are applying new technologies and mindsets to turn the tables on attackers. But as the technologies become more affordable and the models refined, small and medium-sized enterprises can benefit as well.

Small and medium-size organizations can also benefit

Larger organizations with more resources are applying new technologies and mindsets to turn the tables on attackers. But as the technologies become more affordable and the models refined, small and medium-sized enterprises can benefit as well.

4 Build resilience for any scenario

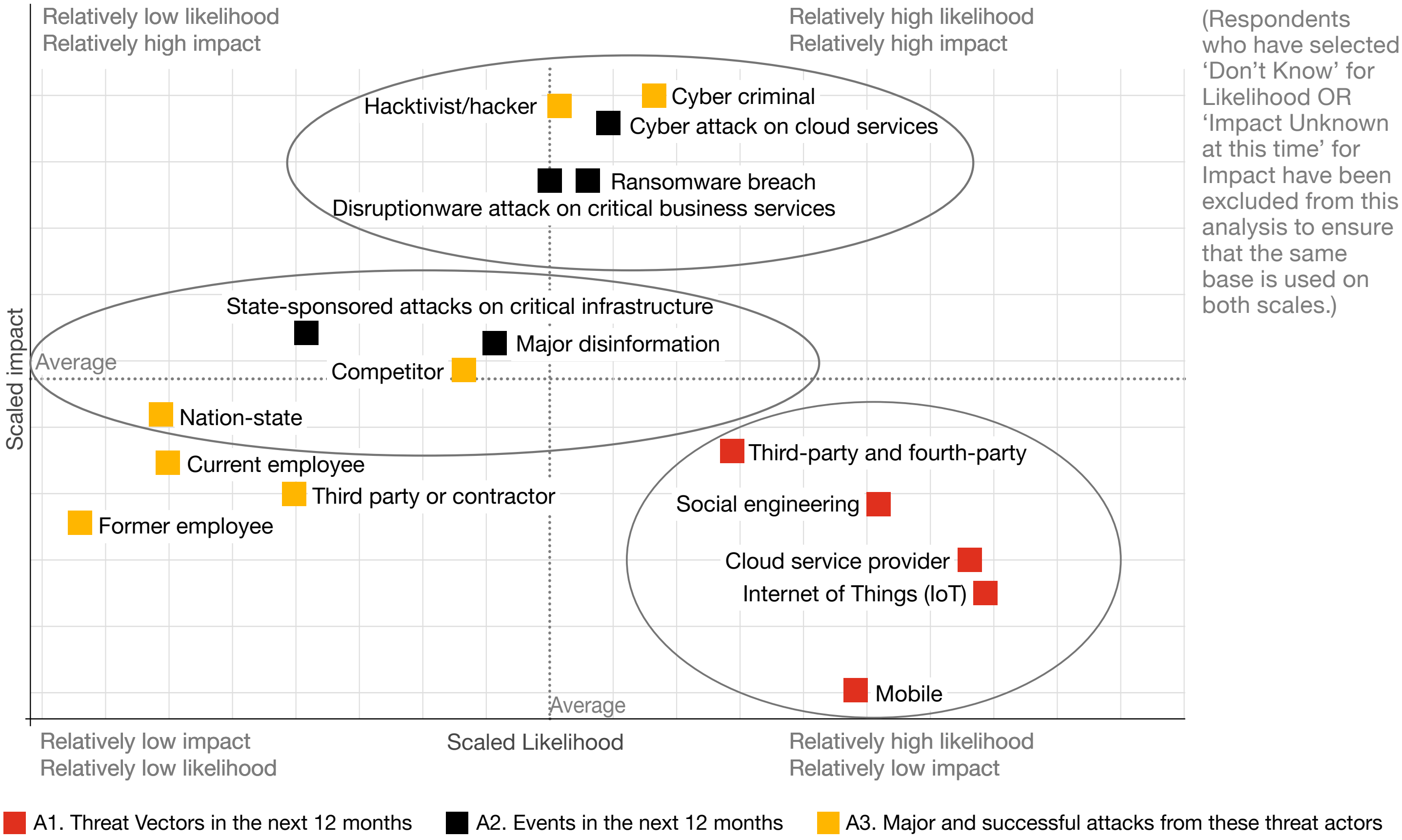
The threat outlook for the next year

In these uncertain times, businesses want certainty. Forty percent of executives in our Global DTI 2021 survey plan to increase resilience testing to ensure that, if a disruptive cyber event occurs, their critical business functions will stay up and running.

The likelihood of cyberattack is greater in 2020 than ever before. The year has brought a surge in intrusions, ransomware, and data breaches, along with an increase in phishing attempts.

We asked executives to rank the likelihood of cyber threats affecting their industry, and the impacts on their organizations, over the coming year. IoT and cloud service providers top the list of 'very likely' threat vectors (mentioned by 33%), while cyber attacks on cloud services top the list of threats that will have 'significantly negative impact' (reported by 24%).

Threats, actors, and events: relative likelihood and impact



(Respondents who have selected 'Don't Know' for Likelihood OR 'Impact Unknown at this time' for Impact have been excluded from this analysis to ensure that the same base is used on both scales.)

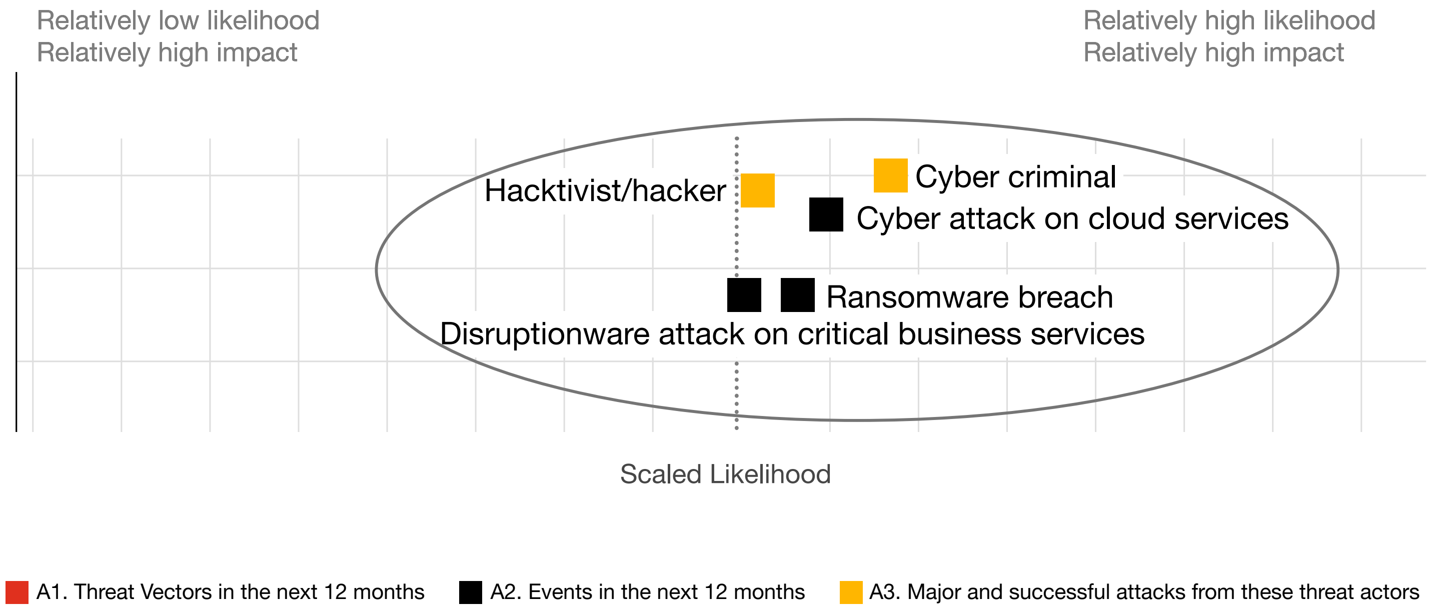
Source: PwC, Global Digital Trust Insights Survey 2021, October 2020: base 3,217
Q: In your view, what is: (a) the likelihood that these threat vectors are going to affect your industry in the next 12 months, and (b) the extent of impact, if it were to happen, on your organization?
Q: In your view, what is: (a) the likelihood of these events occuring in your industry in the next 12 months, and (b) the extent of impact, if it were to happen, on your organization?
Q: In your view, what is: (a) the likelihood of a major and successful attack from these threat actors in your industry in the next 12 months, and (b) the extent of impact, if there was a successful attack, on your organization?

Relatively high-likelihood, high-impact threats

More and faster digitization means an increase in digital threats and potential for harm to the business. Most likely to occur in the next year and potentially most damaging, survey respondents said, are attacks on cloud services, disruptionware affecting critical business services (operational technology), and ransomware. **Are your investments addressing these threats?**

Fifty-five percent say it's likely or very likely that their cloud service provider will be threatened in the next year, 45% say the impact would be negative or very negative. Fifty-seven percent deem an attack on cloud services to be likely, and 59% say the impact would be negative or very negative. A similar number (56%) rate a ransomware attack likely or very likely over the next year, and 58% say the consequences would be negative or very negative.

Cloud providers are attuned to the threats on cloud services: more executives in the technology, media, and telecommunications industry (TMT) assign "very high" likelihood to such threats.



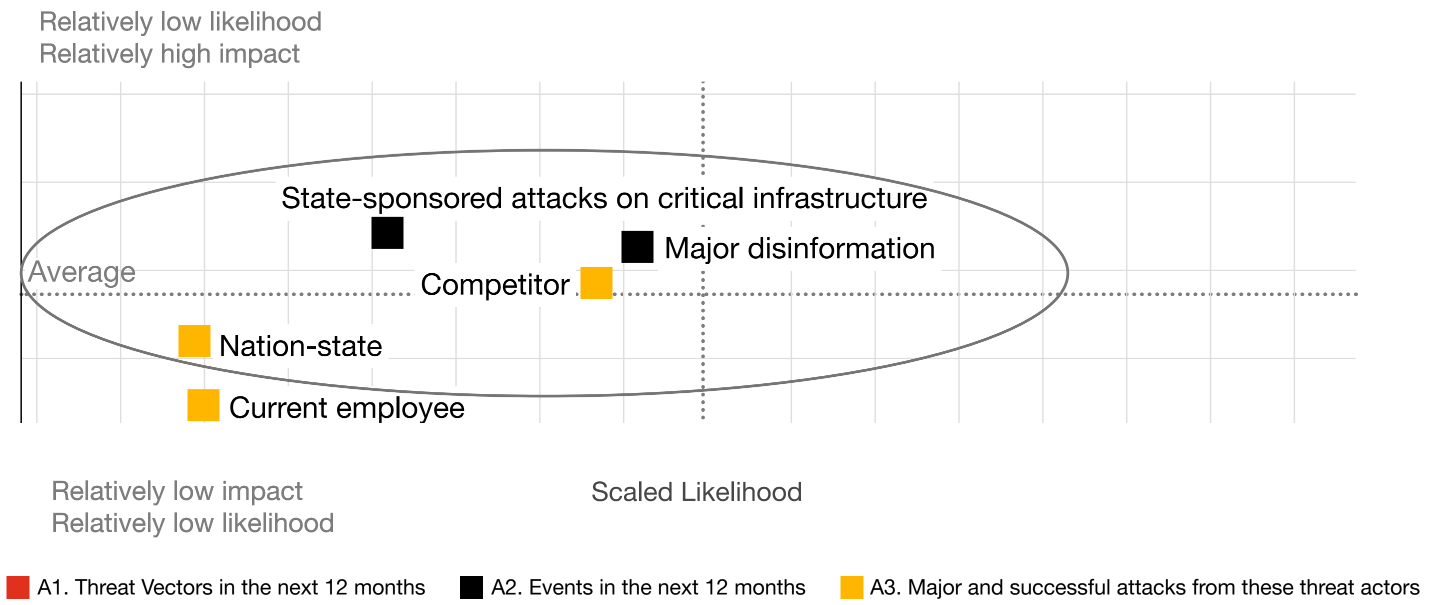
Source: PwC, Global Digital Trust Insights Survey 2021, October 2020: base 3,217

Relatively low-likelihood, high-impact threats

Next, we come to a cluster of threats considered low-likelihood, high-impact. We've been wrong before, however: in the World Economic Forum's Global Risk Report 2020, 'infectious diseases' was deemed an unlikely threat. We can't predict the future; we can only plan for it. Have you tested resilience plans for these kinds of threats?

In this category are disinformation attacks (54% likelihood and negative impact) and threats sponsored by nation-states (48% likelihood, 51% negative impact) and competitors (53% likelihood, 56% negative impact). Executives in industrial manufacturing, financial services (FS) and TMT are particularly attuned to nation-states as threat actors.

A higher proportion of respondents in the Netherlands rated the extent of the impact of key threats (including ransomware, nation-state and insider attacks) as negative compared to the global results, although the likelihood of ransomware was rated lower. This indicates that more of the respondents see their organisations as less resilient to these threats. Companies should prioritise implementing mechanisms to detect, respond and recover from these threats.

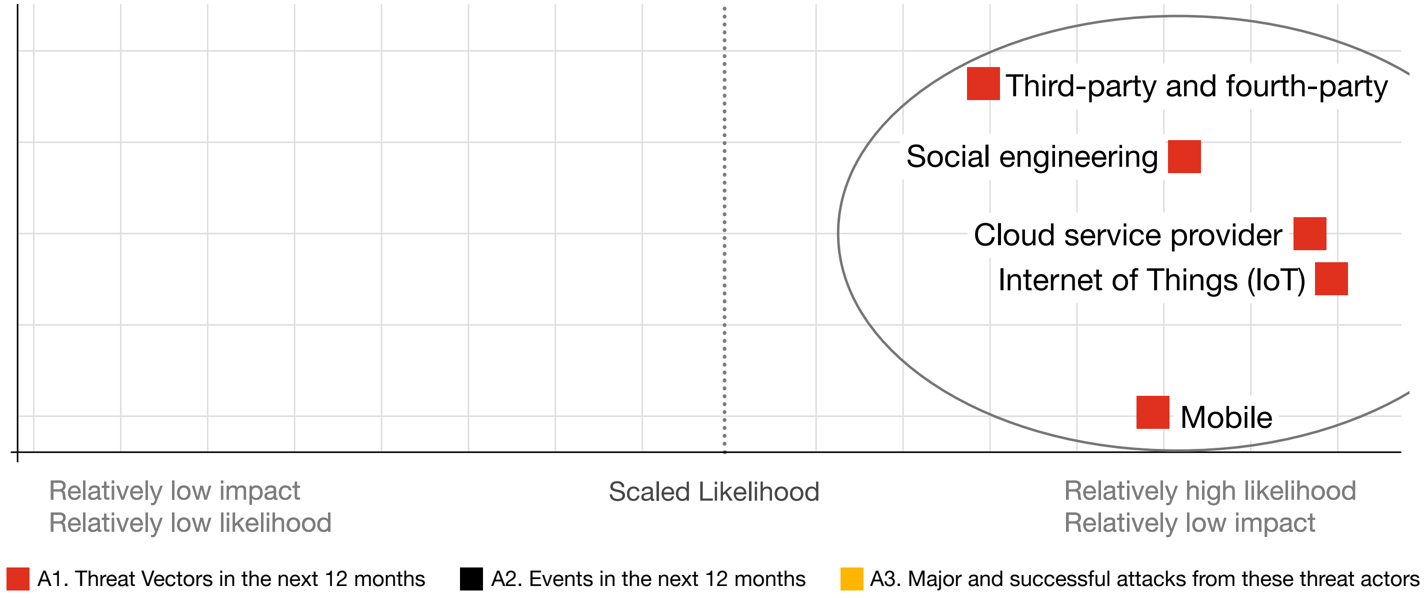


Source: PwC, Global Digital Trust Insights Survey 2021, October 2020: base 3,217

Relatively high-likelihood, low-impact threats

Relatively high in likelihood but lower in impact are ever-present threat vectors, such as attacks via IoT (65% likelihood, 44% negative impact) and cloud providers as well as those posed by third parties (49% likelihood, 52% negative) and social engineering (63% likely but negative impact for just 49%). Health industry executives are particularly concerned about the impact of attacks via third parties.

Good cyber hygiene is imperative to stave off these threats. Talent and tools that harness data in real time to detect threats and respond to them are progressing rapidly.



Source: PwC, Global Digital Trust Insights Survey 2021, October 2020: base 3,217

How ready are you for the coming threats?

More executives in FS, TMT, and health industries think misinformation and ransomware are very likely to occur in the next year. Executives in energy, utilities, and resources are more likely to predict a significant negative impact from almost all threats.

“Cyber Security people have for last twenty years been preaching the choir that it will be a topic on Board of Directors Tables. Now this starts to be finally true and the more our world digitalizes the more integral Cyber Security must be to everything we do. I hope you withstand the pressure this change poses to you….diamonds are made….” says Petri Kuivala, CISO, NXP.

If you were to draw up a likelihood-impact grid containing the cyber threats, actors, and events your organization faces, what would it look like? How is your cyber spending allocated to address these?

More than three-quarters of executives in our Global DTI 2021 survey say that “assessments and testing, done right, can help them target their cybersecurity investments.”

“

Cyber Security people have for last twenty years been preaching the choir that it will be a topic on Board of Directors Tables. Now this starts to be finally true and the more our world digitalizes the more integral Cyber Security must be to everything we do. I hope you withstand the pressure this change poses to you… diamonds are made…

—Petri Kuivala
CISO, NXP

5 Future-proof your security team

Wanted: 3.5 million people for 2021 cybersecurity jobs

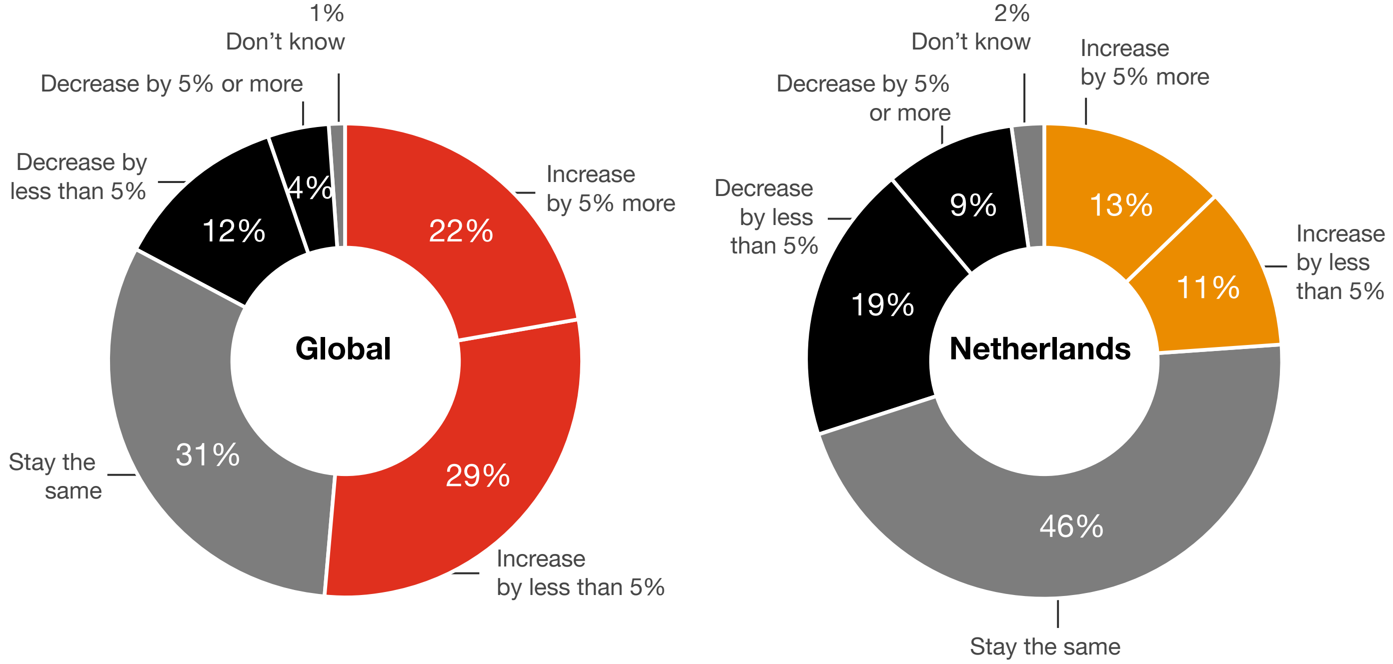
More than half (51%) of executives in our Global DTI 2021 survey say they plan to add full-time cybersecurity personnel over the next year. More than one-fifth (22%) will increase their staffing by 5% or more.

Top roles they want to fill: cloud solutions architects (43%), security intelligence (40%), and data analysis (37%). Cloud security and security analysis are among the skills that a joint ESG and ISSA survey cited as being in shortest supply.

Hiring managers face tough competition in the cyber labor market. The most recent studies indicate that, in the US alone, 50% fewer candidates are available than are needed in the cyber field. Globally, some 3.5 million cybersecurity jobs are expected to go unfilled in 2021.

Only 24% in The Netherlands expect an increase in headcount in the next 12 months, compared to 51% globally. A much higher (46%) proportion in the Netherlands expect their headcount to stay the same compared to 31% globally.

More than half of businesses globally are expanding their cybersecurity teams, but a lot fewer are doing same in the Netherlands



Source: PwC, Global Digital Trust Insights Survey 2021, October 2020: base 3,249
Q: How is headcount for your cybersecurity team changing in the next 12 months?

Hire for 21st-century skills: digital, business, and social skills

In their new hires, more than 40% of executives are looking for analytical skills (47%), communication skills (43%), critical thinking (42%) and creativity (42%). Shaping the future of cybersecurity — one that is in step with the business — means hiring the people who are ready to work collaboratively with others to tackle new, as-yet-undiscovered problems and analyze information.

These in-demand qualities correspond with the expanded role of the CISO as not merely a tech leader, but one who works with colleagues in the C-Suite and the business side to add value overall.

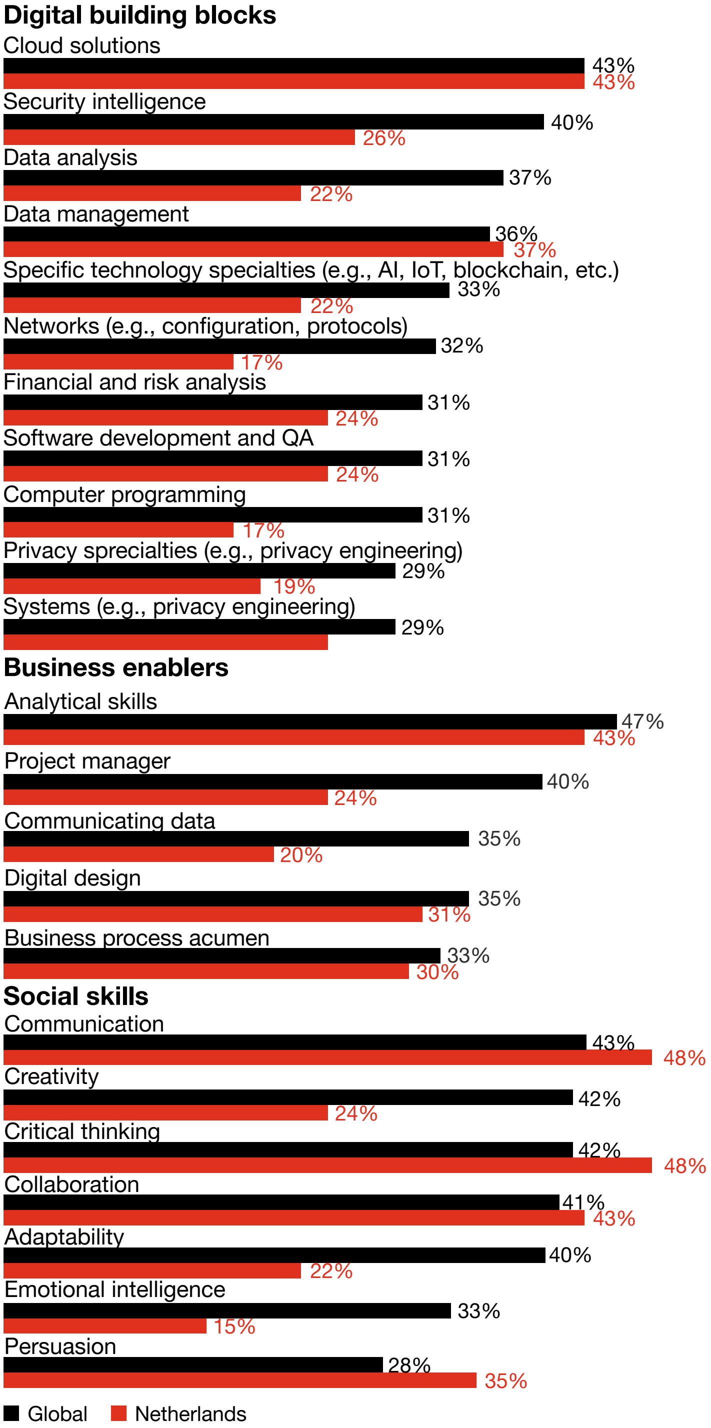
Fewer respondents in the Netherlands require security intelligence and adaptability as skills for a security professional. This might be as a result of the relatively lower ranking of digitisation and cost cutting as an impact due to COVID in The Netherlands compared to the rest of the world. Digitisation and cost cutting certainly require the necessary adaptability.

“Works well with others” is an increasingly important trait for advancement in cyber. CISOs used to look for the person who knew the most about how to configure a firewall or identity and access management, for example. Not anymore. They’ve realized that those skills could be taught a whole lot easier than executive skills. Good communications, good analytical thinking, and the ability to step outside the process and imagine new and better ways to do it — those soft skills are harder to teach.

To attract this new breed of cybersecurity professionals, organizations find the following to be most effective: flexibility, compensation, and training and “cutting-edge projects, technology, and work environment.” Tuition support ranks high with employees in the technology, media, and telecommunications industry, as well.

In the Netherlands, organizations seem to find compensation a less effective tool to attract new talent, as it’s ranked on the 7th place compared to 2nd globally.

New hires need to have digital skills, business acumen, and social skills



Source: PwC, Global Digital Trust Insights Survey 2021, October 2020: base 3,249
Q: Which of the following skills are you looking for in your new hires in the next 12 months?

Hire from within: upskilling 2.0

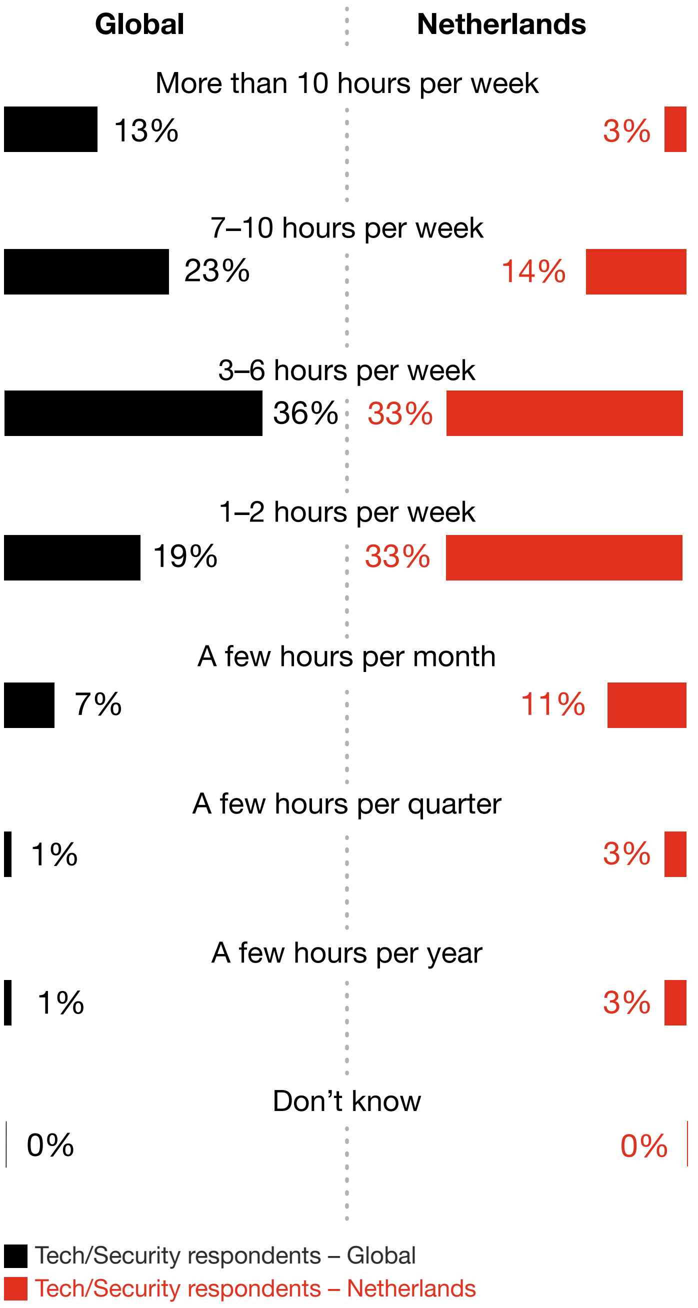
Enterprises feeling the pinch of the cybersecurity skills gap may find much talent in their own backyards, and with only 24% or organizations in the Netherlands expecting headcounts to increase in the next 12 months, internal upskilling is even more important. Organizations are hiring from within, offering upskilling to increase current employees' skills in the same key areas they're hiring for: digital skills, business acumen, and social skills.

Organizations must challenge long-held beliefs about training, and design their programs to be people-powered, business-led, and results-oriented. This approach, which we call upskilling 2.0, uses techniques such as gamification to increase participation, improves effectiveness and recall by having students apply their newfound knowledge towards challenges they face on the job, and rewards progress toward tangible business outcomes.

Executives set a good example: almost three-quarters (72%) of technology/security executives report spending three or more hours per week on work-related learning, and more than one-third (36%) devote more than seven hours per week to learning. Taking courses toward certification and taking online classes are two top ways that executives say they keep pace with fast-evolving developments in tech and cyber, after networking with peers nationally.

Compared to the global results, respondents in the Netherlands reported spending less time on learning and development.

Keeping up with technologies requires significant personal investment in learning



■ Tech/Security respondents – Global
🟥 Tech/Security respondents – Netherlands

Source: PwC Global Trust Insights Survey 2021, October 2020: base 3,249
Q: How much time do you personally devote to learning new things in the technology field that improve the way you do your job?
Tech/Security Respondents Only base: 1,623
Q: How much time do you personally devote to learning new things in the technology field that improve the way you do your job?
Business Respondents only base: 1,626

Access talent through managed services models

Other organizations may not have the resources to compete for cyber talent in this tough market. In such cases, using a reputable managed security services model can help provide companies with a diverse, readily available, highly skilled workforce. The best managed services providers continually invest in hiring, credentialing, and upskilling. They may also have apprenticeship programs that provide their staff with a range of experiences in different industries.

Managed services platforms — networks, the cloud, data, analytical tools, visualization, machine learning — are constantly evolving. By moving to a managed services model, an organization can avoid not only technology investment costs but also the risks that legacy technology poses, including the need for constant upgrades.

An overwhelming majority — nearly 90 percent — of executives use or plan to use managed services. Eighteen percent say they're already realizing benefits from managed services, while 49% are starting to use them, and 18% plan to do so in the next two years.

About the survey

About the survey

The 2021 Global Digital Trust Insights is a survey of 3,249 business, technology, and security executives (CEOs, corporate directors, CFOs, CISOs, CIOs, and C-Suite officers) conducted in July and August 2020. Fifty-five percent of respondents are executives in large companies ($1 billion and above in revenues); 15% are in companies with $10 billion or more in revenues. Female executives make up 28% of the sample.

Respondents operate in a range of industries: Tech, media, telecom (22%), Retail and consumer markets (20%), Financial services (19%), Industrial manufacturing (19%), Health (8%), and Energy, utilities, and resources (8%).

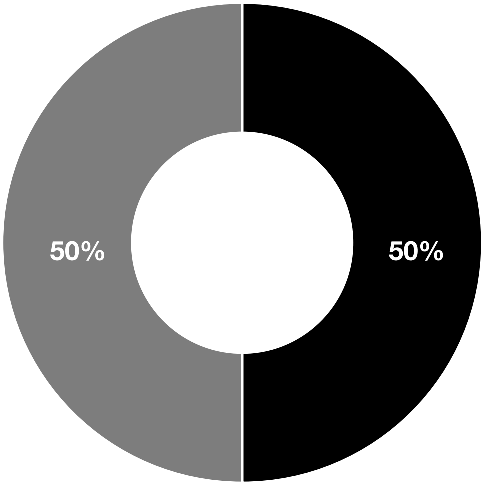
Respondents are based in various regions: Western Europe (34%), North America (29%), Asia Pacific (18%), Latin America (8%), Eastern Europe (4%), Middle East (3%), and Africa (3%).

The Global Digital Trust Insights Survey is formally known as Global State of Information Security Survey (GSISS).

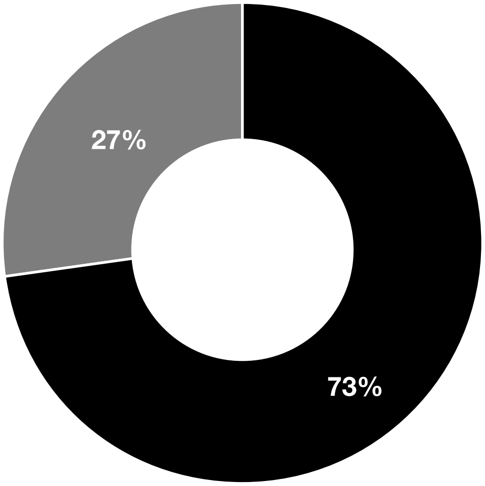
PwC Research, PwC's global Centre of Excellence for market research and insight, conducted this survey.

Job title

Global



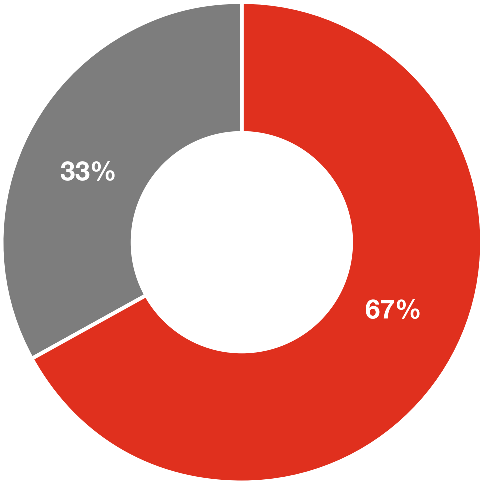
■ Net: Tech/security respondents
■ Net: Business respondents



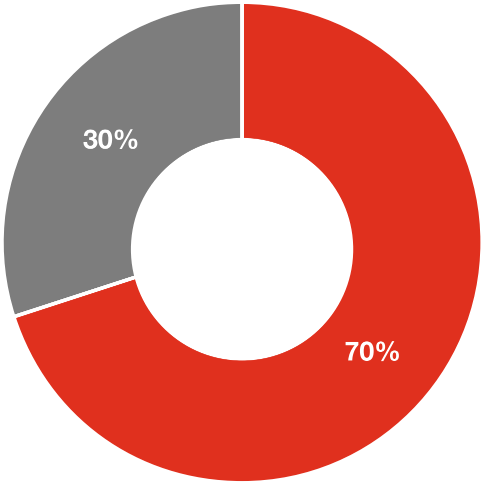
■ Net: C-suite
■ Net: Non C-suite

Chief Executive Officer (CEO)/ President/Managing Director	**21%**
Chief Information Security Officer	**10%**

Netherlands



🟥 Net: Tech/security respondents
■ Net: Business respondents

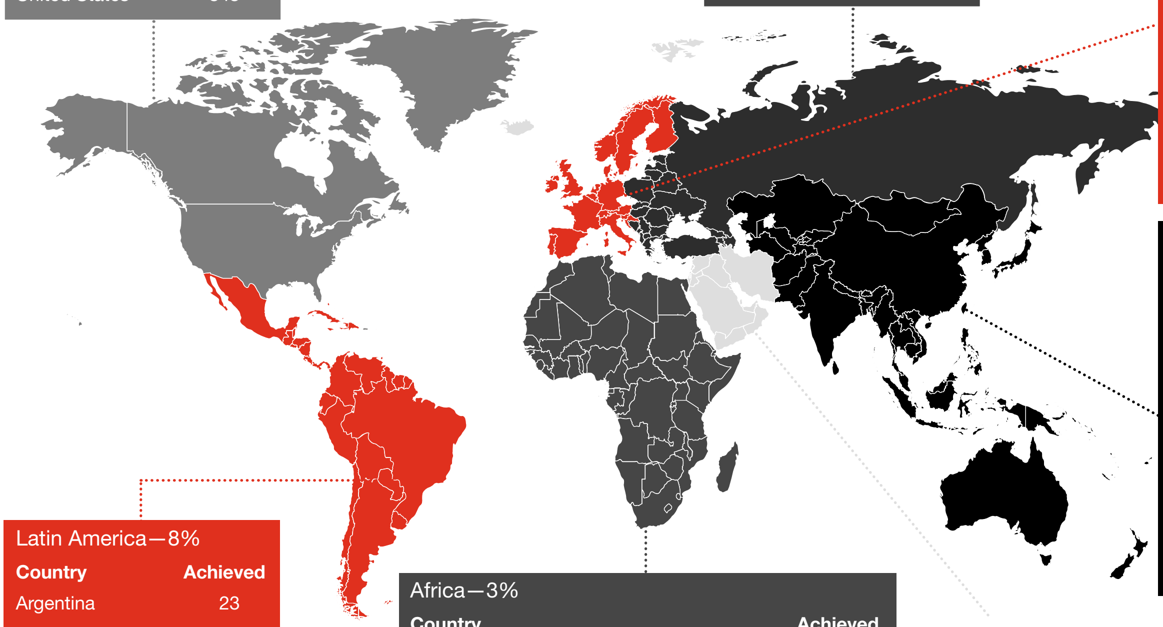


🟥 Net: C-suite
■ Net: Non C-suite

Chief Executive Officer (CEO)/ President/Managing Director	**?%**
Chief Information Security Officer	**?%**

Source: PwC, Global Digital Trust Insights Survey 2021, October 2020: base 3,249
Q: Choose the title that best describes your role.

Region



North America—29%

Country	Achieved
Canada	100
United States	843

Eastern Europe—4%

Country	Achieved
Romania	5
Russia	125
Ukraine	7

Western Europe—34%

Country	Achieved
France	188
Germany	263
Ireland	30
Italy	100
Netherlands	54
Spain	100
Sweden	40
Switzerland	56
United Kingdom	265

Asia Pacific—18%

Country	Achieved
Australia	100
China & Hong Kong	133
India	110
Indonesia	31
Japan	100
Korea	30
Malaysia	30
New Zealand	30
Singapore	31

Latin America—8%

Country	Achieved
Argentina	23
Brazil	109
Colombia	20
Mexico	120

Africa—3%

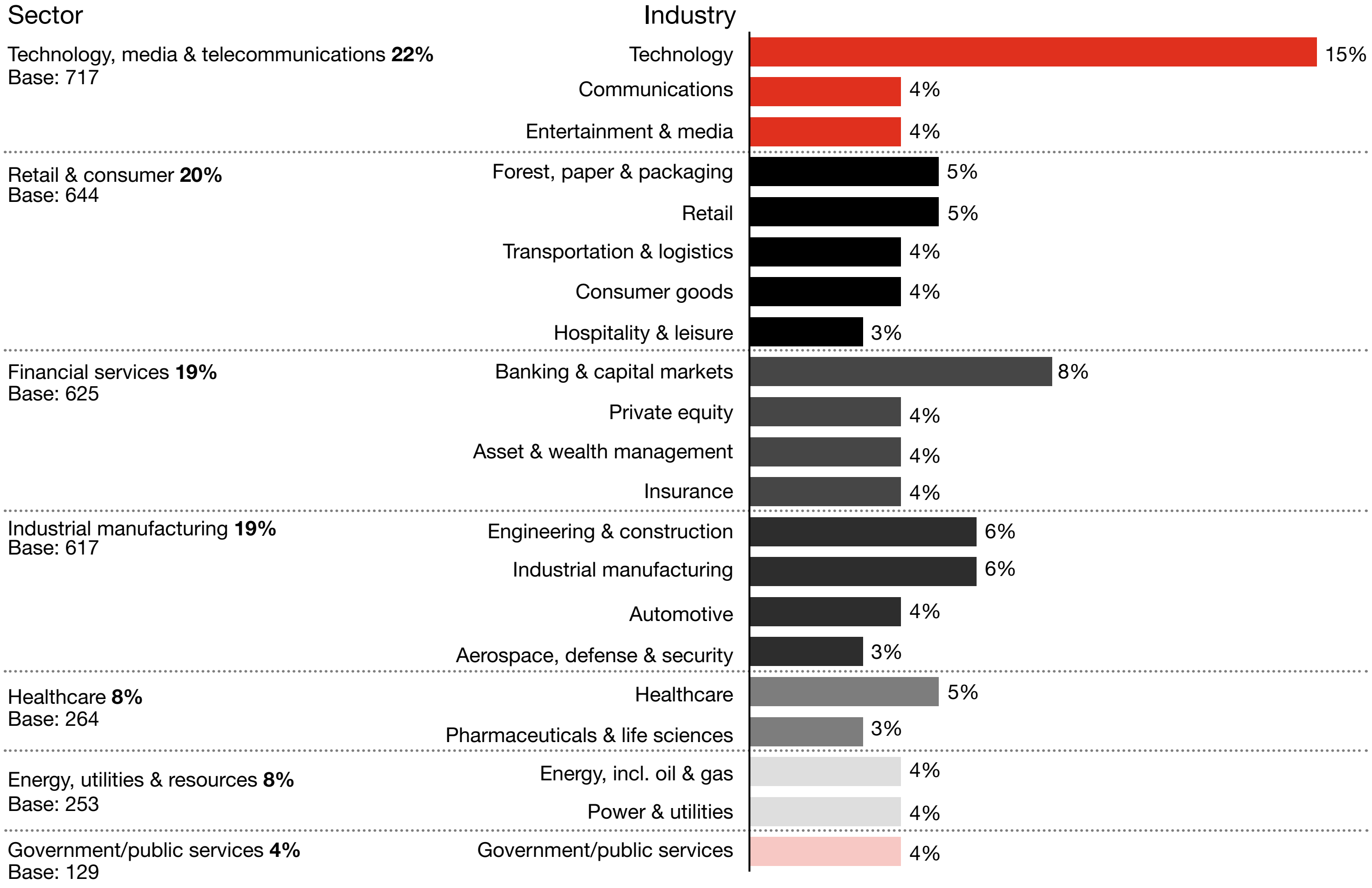
Country	Achieved
East Africa (Kenya, Uganda, Tanzania)	18
South Africa	51
Southern Africa (Botswana, Malawi, Namibia, Zimbabwe)	5
West Africa (Nigeria, Ghana)	31

Middle East—3%

Country	Achieved
Bahrain	10
Kuwait	10
Oman	10
Qatar	10
Saudi Arabia	30
UAE	31

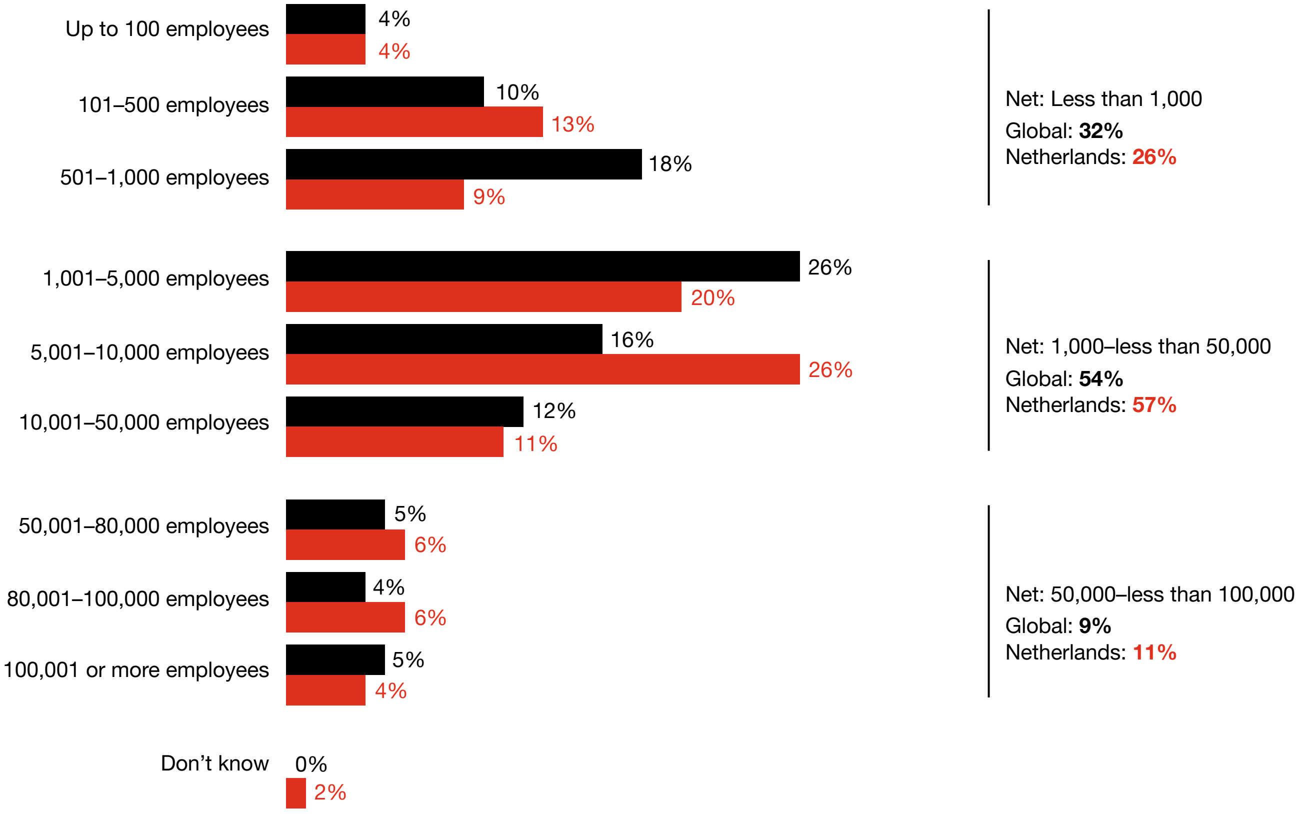
Source: PwC, Global Digital Trust Insights Survey 2021, October 2020: base 3,249
Q: In which country do you primarily work?

Industry



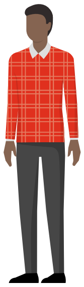
Source: PwC, Global Digital Trust Insights Survey 2021, October 2020: base 3,249
Q: Within which industry does your company mainly operate?

Employee size and gender



Female
Global: **28%**
Netherlands: **22%**

Male
Global: **71%**
Netherlands: **78%**



Other
Global: **0%**
Netherlands: **0%**

Prefer not to say
Global: **0%**
Netherlands: **0%**

Source: PwC, Global Digital Trust Insights Survey 2021, October 2020: base 3,249
Q: How many employees does your organization have globally?
Q: What is your gender?

Contacts

Angeli Hoekstra
hoekstra.angeli@pwc.com
Cybersecurity Partner,
PwC Netherlands

Bram van Tiel
bram.van.tiel@pwc.com
Cybersecurity Partner,
PwC Netherlands

Sergio Hernando
sergio.hernando@pwc.com
Cybersecurity Partner,
PwC Netherlands

pwc.com