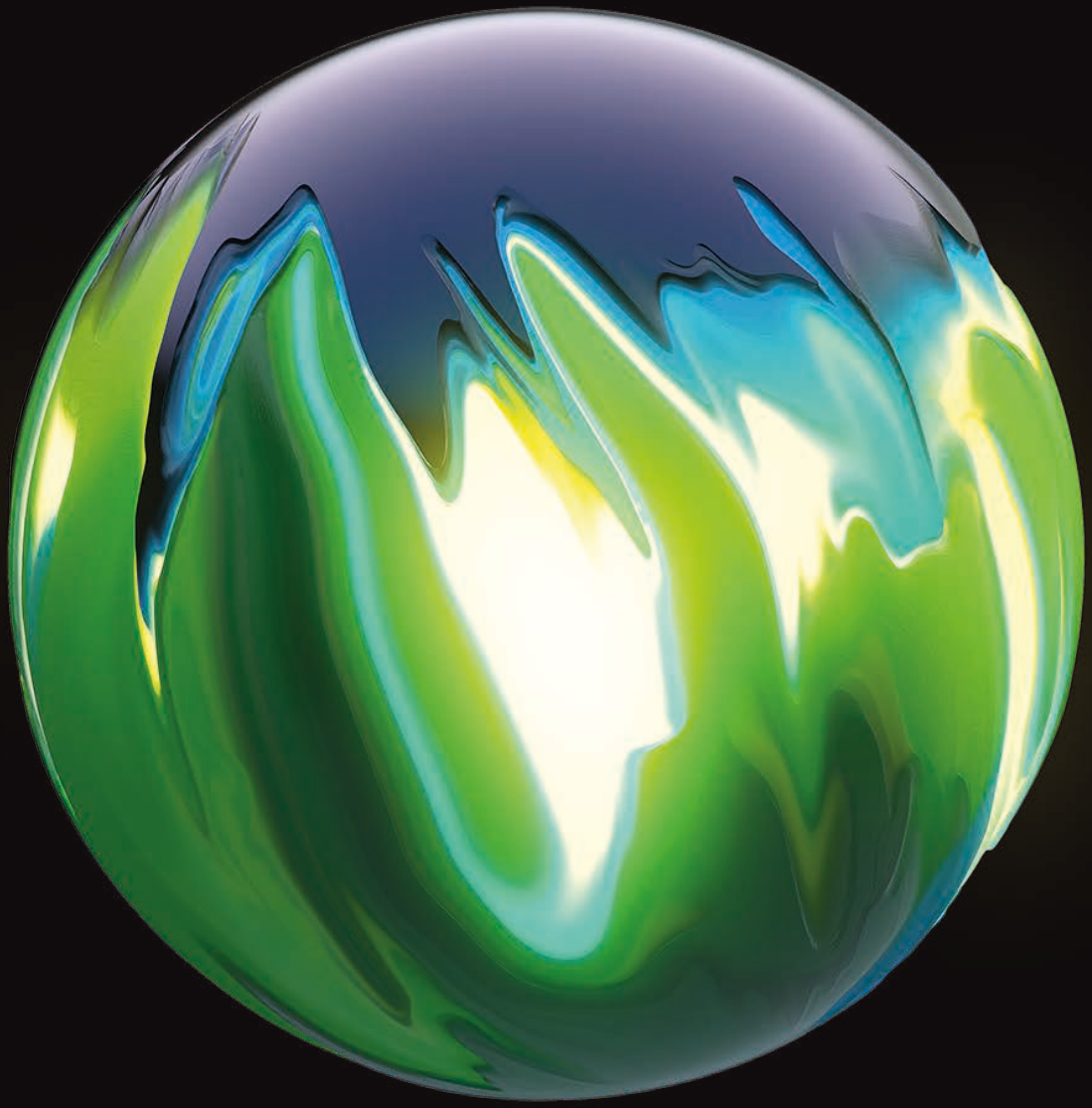
Deloitte.



Cyber security in the Netherlands: a responsibility we share

Progress towards a Dutch cyber security ecosystem

SURVEY AMONG MORE THAN 500 CYBER SECURITY PROFESSIONALS IN THE NETHERLANDS

MAKING AN IMPACT THAT MATTERS since 1845

"We need to exchange knowledge and collaborate together in order to keep our Dutch digital hub safe, to protect the privacy of our stakeholders and to safeguard the very functioning of our society."

Niels van de Vorle
Partner Cyber Risk Services

Preface

In just a few decades, digital technology has changed our world beyond recognition, delivering a fabulous array of benefits. This certainly applies for the Netherlands. We have grasped the opportunities offered by digitalisation to consolidate our role as a major financial, digital and trade hub for the global economy. Just look, for example, at our central role in global high-frequency trading on financial markets. Our global champion in semiconductor technology. Our highly efficient, highly automated port of Rotterdam.

Success comes at a price, however: the digital infrastructure we have built has become far too important to fail. By targeting payments, supply chains and utilities, cyber criminals can bring society to a standstill. The number of ransomware attacks has been rising steadily in recent years, shutting down dozens of organisations in the Netherlands, from local authorities to service providers and from universities to logistics and transportation companies. They give us just a taste of the impact of a cyber attack and the chaos it can cause. Besides ransomware attacks, supply chain attacks are also becoming increasingly common. All this illustrates how relatively easy it still is to compromise our digital infrastructure. Keeping the digital infrastructure secure is a huge responsibility shared by various stakeholders."

The general domain of security used to be up to the government, but national governments lack the reach to effectively counter threats in a globalised world – let alone in cyberspace. Keeping our systems and data safe also requires the engagement of businesses and other organisations. Accordingly, we have seen cyber security rapidly climb the agenda of organisations across the public and private sector, a trend driven either by their CISO or by arising business necessity.

But how do we ensure that all these parties maximise their impact and avoid reinventing the wheel? In other words, how do we shape the future of cyber security? This is a complex task, which we can only accomplish by collaborating together. Deloitte has taken up the challenge to make this happen here in the Netherlands. Our experts strive to connect government, businesses and citizens in ecosystems and translate security challenges into solutions to future-proof our country's cyber security. Deloitte is actively collaborating in the cyber security ecosystem with public and private parties.

In fighting cybercrime, however, it's essential to maintain the trust of stakeholders and society as a whole. Trust is the cornerstone of every relationship. It's the foundation of each interaction an organisation has with employees, vendors, supply chain partners, customers and the broader community. From this basis of trust, the ways organisations work, collaborate and engage with stakeholders remain sustainable and secure as they grow. Losing that trust means losing their license to operate. Therefore, security must be designed to respect privacy and other basic rights. This, too, is an area where Deloitte has deep expertise and great ambition. This is part of our broader goal to help organisations become more responsible in doing business.

In this ecosystem, we envision that organisations learn and progress by engaging in an ongoing discussion. To provide useful input for that discussion, we have performed a sweeping study into cyber security practices across our country, polling 544 respondents (comprising of 70% CxOs and 30% holding various other information technology and management positions). While the importance of cyber security is universally felt, the approach to cyber security challenges is extremely varied. The differences between sectors, between large and small organisations and between seniority levels within organisations show that there is much to be gained by learning from each other. And the fact that so many have taken part in the survey reflects a willingness to do so.

This report is a must-read for leaders who manage cyber security challenges, but let's do more than just read it. Now is the time to take our conversations on cyber security to the next level. We need to exchange knowledge and collaborate together in order to keep our Dutch digital hub safe, to protect the privacy of our stakeholders and to safeguard the very functioning of our society.

Niels van de Vorle
Partner Cyber Risk Services

Contents

Executive Summary

Cyber security is continuously in motion. It has to be in order to keep up with constantly changing cyber threats. At Deloitte, we were keen to know where Dutch organisations currently stand with respect to cyber security. What they are worried about, what their goals are, and what is needed to achieve success. How they see the future. And above all, their thoughts on making the Dutch digital ecosystem safer.

1. The ultimate goal of cyber security

25% of the respondents believe the ultimate goal of cyber security is to protect people and assets from harm, misuse and abuse. **22%** opined that protecting the vital assets of the company is the most important objective. For at least **one out of ten**, the ultimate goal of cyber security is making the digital ecosystem a safer place.

"The Financial Sector agreed not to compete on cyber security years ago. Instead, banks are sharing information and helping each other with best practices. Other sectors have been following this example. By doing so, all can offer clients, themselves and society the best possible protection."

- Kevin Jonkers, Director Cyber Risk Services

2. Strategy

92% of organisations stated to have an up-to-date cyber security strategy, which (based on our survey) is usually a separate annual plan with a roadmap (**80%**). Conversely, **6%** of organisations are starting to set up their strategy, while **15%** are already working on a next-level mature strategy. The most frequently cited success factors for achieving cyber security goals are increased operational excellence, clear cyber security communication, training the organisational workforce to become more aware of cyber security matters, and meeting various compliance requirements. Meanwhile, organisations seem to struggle to mitigate all cyber threats and invest in every single department, thus, the general practice is to make calculated choices and strengthen their most important and valuable business areas and controls.

"A cyber security strategy must first be realistic and workable for the rest of the organisation. For next-level maturity, it must be embedded in primary processes and the overall strategy."

- Robbin van den Dobbelsteen, Director Cyber Risk Services

3. Cyber security on the executive board's agenda and the allocation of cyber security budget

42% of executive boards discuss cyber security at least every quarter, but **25%** of them do so once a year or less. The survey shows that the larger the organisation is, the more frequently cyber security is discussed at board level. Comparing sectors, providers in Financial Services are champions in board-level engagement on this topic, while public sector awareness is significantly lower. Interestingly, our survey shows that for an average of **8%** of our CxO respondents the ultimate goal of cyber security is not always clear.

"If CISOs start focusing more on securing emerging technologies, they can act as business enablers and strengthen the position of the company compared to competitors."

- Dana Spataru, Partner Cyber Risk Services

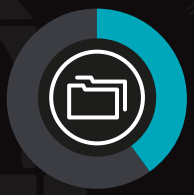
Our survey shows that **61%** of organisations allocate up to **11%** of the information technology budget to cyber security, and **73%** of organisations increase this budget annually, although not exceeding **15%** on an annual basis overall. If we compare sectors, cyber security budgets are relatively high in the Energy, Resources & Industrials sectors and among Life Science & Healthcare organisations, while **43%** of the Public Sector do not know exactly how much they actually spend on cyber security.

"Cyber security budgets are not unlimited, especially in Small and Medium-sized Enterprises, so you have to understand where your investments will be most impactful and make choices."

- Jurrien Mammen,
Partner Cyber Risk Services

4. Deep diving into our most commonly feared threats

Part of our survey focused on anticipated developments in cyber security, (potential) cyber threats and the organisation's confidence in handling them. **The most commonly feared threats are:**



data leakage (**40%**)

phishing, malware, or vulnerability exploits (**35%**)

extortion or destruction of the organisation's data (**25%**)

The largest organisations (>10,000 employees) have an above-average fear (**27%**) of security breaches involving third-party organisations.

"I don't believe digital threats are becoming more sophisticated overall, as easy hacks are still effective and lucrative. It's organisations themselves that are becoming more complex and losing track of their vulnerabilities."

- Frank Groenewegen,
Partner Cyber Risk Services

In case of a ransomware attack, less than a third (**30%**) of the respondents are sure they would pay to get their data back. But opinions vary widely on this topic. The positions that most often choose to pay are CEO, CIO, and CRO (**52%**, **48%** and **46%** respectively), while **29%** of CISOs would pay. Large organisations are also less likely to pay, with only **15%** of organisations with 10,000 employees or more agreeing with this statement. The same is true for organisations in the Public Sector; only **17%** believe that paying is the best option, while organisations from Financial Services (**40%**), Technology, Media & Telecommunications (**38%**) and Energy, Resources and Industrials (**38%**) are more convinced.

5. The development of the CISO role

Nowadays CISOs predominately report to the CIO (**49%**) where only **13%** report to the CFO. **Our survey shows that the three challenges most felt by CISOs are:**

managing too many organisational priorities simultaneously (**31%**)

lack of integration of cyber risk priorities with business priorities (**28%**)

inadequate governance across organisation (**26%**)

"The role of the CISO is changing from being perceived as 'the department of no' to being a business advisor and enabler. A CISO no longer needs to rely on a deep technical background. It's more important to be a people person."

- Martijn Knuiman,
Partner Cyber Risk Services

6. Towards a Dutch cyber security ecosystem

63% of respondents from large organisations with more than 10,000 employees see opportunities to contribute to a more resilient sector and a safer digital ecosystem. The surveyed CISOs leave little room for interpretation: **100%** of these respondents agree with this statement. The creativity, confidence and positivity in this regard seems to grow with organisation size. **These results highlight the evolution towards a safer and more resilient digital society**.

"We need to exchange knowledge and collaborate together in order to keep our Dutch digital hub safe, to protect the privacy of our stakeholders and to safeguard the very functioning of our society."

- Niels van de Vorle,
Partner Cyber Risk Services

Methodology

Deloitte Cyber Risk Services, in conjunction with **Markteffect** (one of the leading market research companies in The Netherlands), polled 544 professionals who oversee cyber security at organisations in an online survey. Those professionals are CISO (19%), other CxO-level executives (51%), and professionals holding various other information technology positions (30%), working across six different sectors: Financial Services (13%), Energy Resources & Industrials (13%), Technology, Media & Telecommunications (30%), Consumer (17%), Public Sector (20%) and Life Sciences and Healthcare (4%). The organisations they work for range in size from up to 1,000 (60%), 1,000 to 5,000 (19%), 5,000 to 10,000 (6%) to more than 10,000 employees (15%). The fieldwork took place between September and December 2020.

Note: *The graphs in this report show rounded figures. Due to rounding differences, it may happen that they add up to 99% or 101%.*

1. Organising cyber security

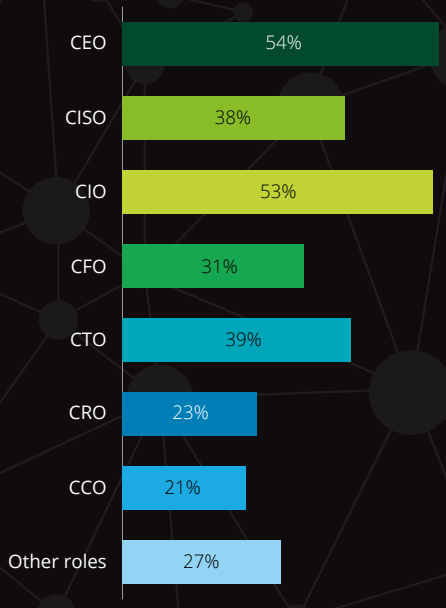
Organising cyber security
A Deloitte perspective by Jurrien Mammen

Jurrien, partner Deloitte Cyber Risk Services, has over 20 years of experience in risk and strategy consulting and currently leads the Dutch Cyber Strategy Team.

"The survey looks at how often the board discusses cyber security, but more discussion isn't necessarily better. Indeed, a significant percentage of respondents (54% of CEOs, 38% of CISOs) say that their board doesn't have a current and accurate understanding of the cyber landscape. On the other hand, where cyber security is well organised and understood, it hardly needs discussion at all. What interests me more is the quality of that discussion. Are the right issues being discussed? Are tough questions being asked? Like, whether the people taking the decisions know enough about the subject and the latest threats. Or whether product innovation teams keep cyber security in mind. Whether the right investments are being made.

Talking about investments, the survey shows that cyber security budgets are significant and growing. But here, too, more budget is not necessarily better. The survey shows that 31% of CFOs realise that understanding the areas where security investments are most impactful is important to being successful. Unsurprisingly, then, some 40% of respondents feel that protecting everything is unaffordable, and have made choices as to what to recover and what to let fail.

% of respondents that agree with the statement: 'The Executive Board of my organisation doesn't have a current and accurate understanding of the cyber landscape':



Cyber security is indeed costly, and as threats increase in sophistication and number, there's a risk that further investment isn't economically feasible, especially for smaller organisations. So either they achieve more effective cyber security for the same price, or they go out of business. This may explain the trend we see among smaller players to insource cyber security. Either to save costs, or because they cannot find an external party willing to serve them, given their tight budget.

Among these smaller organisations, 39% see cyber security as their own responsibility. In my view, the government also has a responsibility to make the overall operational environment safer, for example, by taking higher-level measures to reduce the attack surface, or by stimulating innovation and providing shared infrastructure. Larger organisations (50%) realise that cyber resilience is a responsibility they share with the government. They are aware of the fact that combating cyber threats effectively requires stakeholders from various domains (e.g. Cyber Crime and Fraud).

In the past year, working from home has erased a lot of status and hierarchy. The way we organise work today is much more fluid and adaptive, accelerating knowledge sharing, both within and between organisations. Today's CISOs can be more agile in responding to immediate threats, and instead of big projects, they'll be handling more projects, but smaller ones."

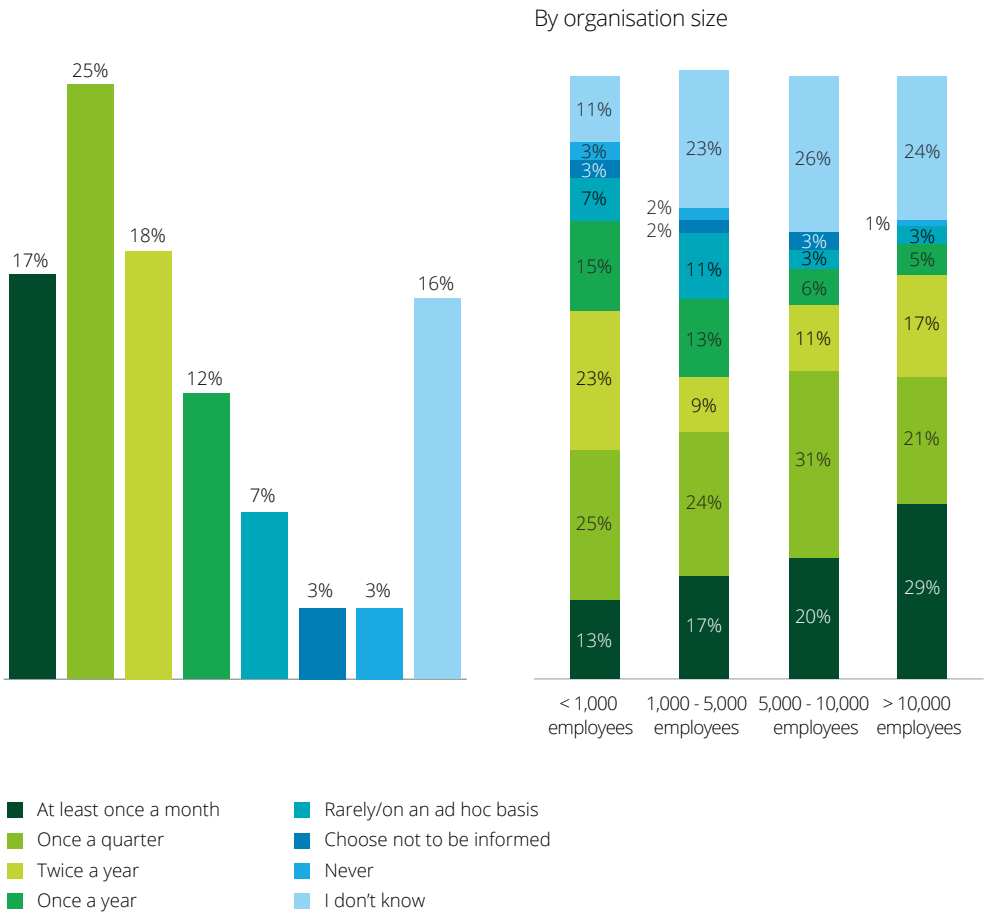
In our survey, we asked questions on how often cyber security is discussed in the executive board, and how much budget is allocated to cyber security related to the overall IT budget.

1.1 Cyber security discussed in the executive board

Cyber security appears to be fairly well on the radar of executive boards. Cyber security is discussed at least every quarter at 42% of the organisations, while 17% of executive boards discuss cyber security at least once a month. And yet, at 13% of the organisations cyber security is rarely to never discussed in the board room. Larger organisations seem to include cyber security more frequently in their executive board's agendas, compared to mid-sized and smaller organisations.

- 29% of the large organisations (with > 10,000 employees) discuss cyber security at least once a month; however nearly 2 out of 5 are unaware of the frequency.
- About a quarter of the organisations with 1,000-5,000 employees discuss cyber security related matters once a quarter, while in the category 5,000-10,000 over a third agree with this statement.

How often is cyber security a subject in the executive board?



1.2 Cyber security budget: the trend of the spend

Allocating sufficient budget is an important factor for success in any field of activity, and this is also true for fighting and defending against (potential) cybercrime. 63% of our survey's respondents are of the opinion that you need to **constantly invest** in the most advanced technology if you want to mitigate cyber risks. This is partially due to a rapidly changing cyber environment.

Within large organisations (> 1,000 employees), cyber security budgets seem to range from 3% to 11% or more of the total IT budget, where about 40% of this group are unaware of the cyber security budget's share.

Further specifying the allocation of cyber security budget by industry, the graph below presents us with the following:

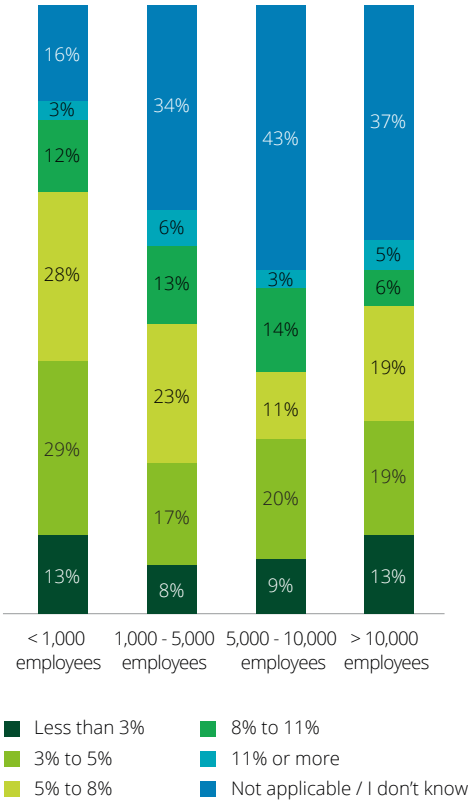
- At least 50% of organisations across Financial Services, Consumer, Telecom, Media & Technology and Energy, Resources & Industrials spend 3%-8% of their IT budget on cyber security.
- 17% of Energy, Resources & Industrials and Life Science & Healthcare organisations spend 8%-11% of their IT budget on cyber security – which is slightly higher if compared to organisations in other sectors.
- 43% of public sector organisations are currently not aware of their cyber security budget.

"Budget doesn't indicate how secure a company is. Compliance-based frameworks also have their limitations. In fact, success and maturity in security are very hard to measure."

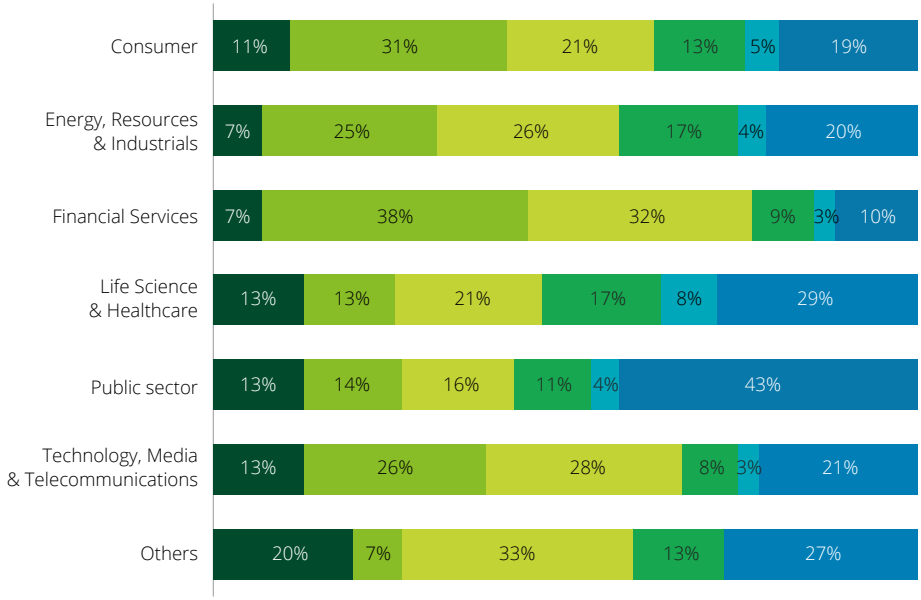
- a respondent

Cyber security budget as percentage of the overall information technology budget

By organisation size



By industry



Development of security budget year-on-year

Cyber security budgets seem to be rising steadily year-on-year:

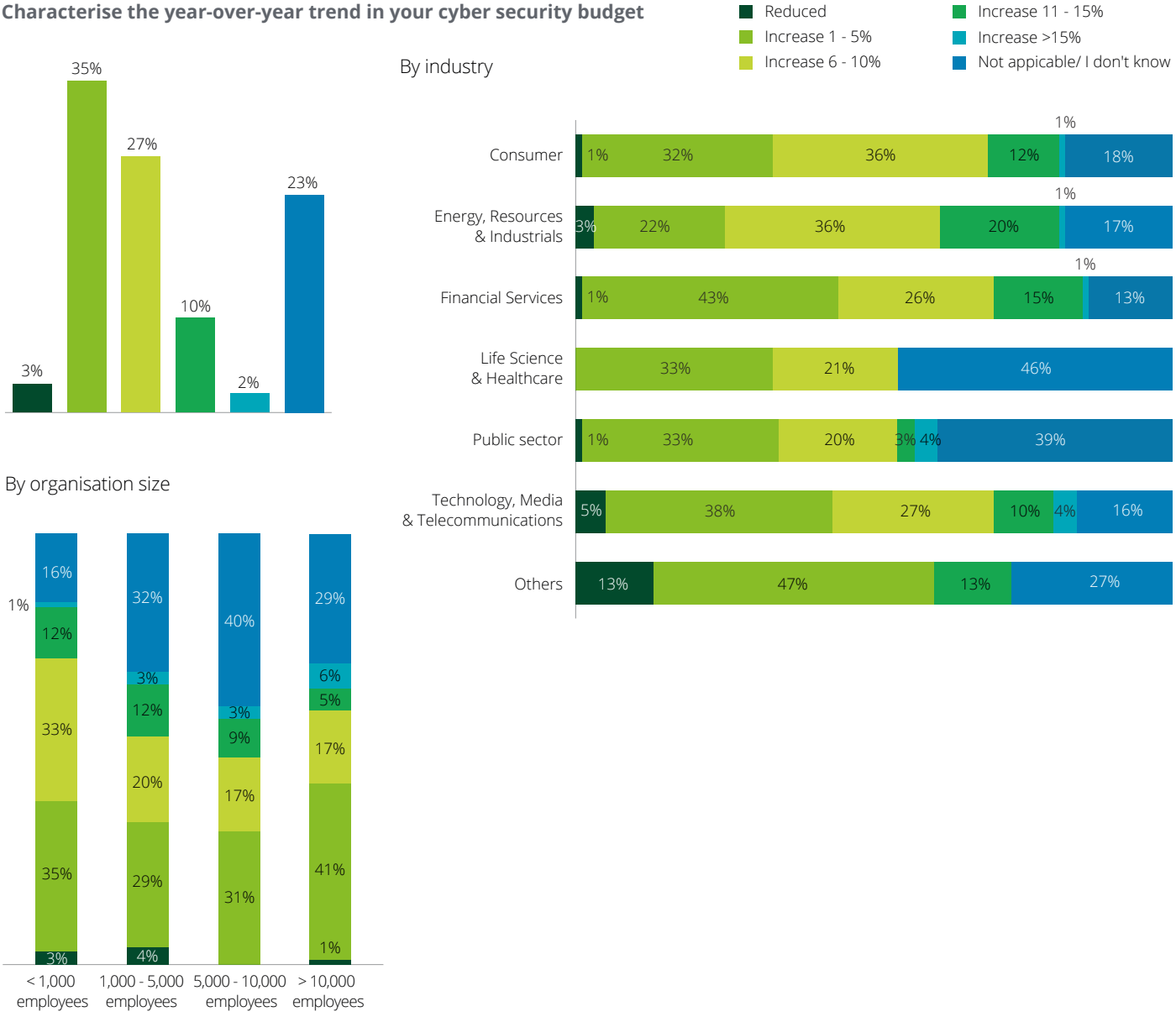
- 35% of our survey respondents said that the annual security budget had grown by 1% to 5%.
- 27% of organisations have seen a larger increase of 6% to 10%.
- 12% of organisations saw their cyber security budget increase by 11% or more.

More interestingly, if we take a closer look into characterising the year-over-year trend by industry, we see that organisations from Financial Services, Energy, Resources & Industrials and Consumer witnessed an overall higher year-over-year growth in their cyber security budgets (up to 15%) compared to organisations in other industries.

Only 3% of the respondents said their cyber security budget had decreased compared to last year. They also indicated the reasons for this, which were mostly because their organisation had been forced to reduce its total costs.

Moreover, as society and organisations have been affected by COVID-19 they need to prepare for the potential aftermath. Our surveys show that surprisingly enough, only 8% of CISOs of organisations bigger than 1,000 employees fear that COVID-19 is a threat to the prioritisation of cyber-related investments.

Characterise the year-over-year trend in your cyber security budget



Embracing emerging technologies
A Deloitte perspective by Dana Spataru

Dana, partner Deloitte Cyber Risk Services, currently leads Deloitte's Global Emerging Technologies security team. Her focus on emerging technologies brings new perspectives to digital transformations, where secure products and processes create new value streams and enable future growth.

"Security can be a business enabler and active driver of future growth. For this to happen, though, CISOs must take emerging technologies into consideration. "Emerging technologies" is a label applied to relatively new technologies such as connected products, cloud, 5G, and brownfield areas such as operational technology. Traditionally, emerging technologies have not been part of security strategies, but they are now increasingly converging with IT.

Instead of reaping the benefits of emerging technologies, some CISOs still struggle with them and view them as complicating factors. 10% of CISOs in our research indicated that emerging technologies give them headaches.

The term "emerging" might be confusing in this context, as these technologies are not really emerging but are already here. Clients today use emerging technologies to improve operational efficiency, increase health and safety, boost automation and reduce costs. And those are only some of the benefits. Telecom organisations are developing new 5G-based products and services, and manufacturers have developed many connected products or have enriched their existing machines with connectivity.

If CISOs turn their focus on securing these new aspects of business, they can act as business enablers and strengthen the position of their companies vis-a-vis competitors. If CISOs address privacy and security risks more proactively, they can give their organisation's business side more confidence to venture into these novel areas.

This discussion should start in the boardroom. Our research shows that cyber security is discussed in the boardroom at a minimum of once per quarter in only 42% of organisations. This means that CISOs at the other 58% have work to do. This topic should be on the agenda at least monthly. If CISOs don't move quickly, they will be cut out of the digital decision-making of other departments.

This would be a missed opportunity. Organisations can look at security and design their future growth paths in an integrated way. What we often see is that manufacturing departments who use new technologies are already making decisions about their own security, and that digital departments run their products with their own established security processes. While it's positive to see that security measures are being embedded, if security is siloed, it's hard to learn from the experiences of other business units. These organisations are likely duplicating costs and efforts. More collaboration and clear governance are required between IT security, manufacturing security and product security to manage security risks and capitalise on opportunities.

The role of a CISO should be to share his or her experiences and connect the dots in a security strategy that covers the entire organisation. A good example is using security as a driver for increased operational efficiency and cost reductions, which in turn covers the cost of security. We recently implemented an integrated security operations centre at a large pharmaceutical company. This centre helps to increase automation and operational efficiency while decreasing health and safety risks in the manufacturing environment. It also creates products with embedded security and privacy, while simultaneously covering the costs of security. This helps the CISO to get buy-in from—in this specific case—manufacturing teams.

There's much we can learn from the most successful digital organisations — not just the tech giants but also the upcoming technology companies offering only digital products and services. They have built-in security in the core of their products, because they know that if they don't, they won't sell them. They have coupled security KPIs to business KPIs because they are inextricably linked.

Our research shows that the role of the CISO is developing in the right direction: from a purely technical to a more business integrated role. In the coming years, I hope this development accelerates, and that CISOs get and take the position they deserve."

2. Moving up the maturity curve

Moving up the maturity curve
A Deloitte perspective by Robbin van den Dobbelsteen

Robbin, director Deloitte Cyber Risk Services, has been advising on cyber security for 15 years, and has fulfilled several CISO positions on an interim basis with larger global organisations.

"It's good to see that almost every respondent's organisation has a cyber security plan, but whether it's effective depends on the **perspective** it was written from. A plan solely written by cyber security experts is likely to be quite short, directive and focused overwhelmingly on risks, rules and sanctions for non-compliance. However, no matter how sensible the rules are, they must also be **realistic and workable** for the rest of the organisation. Otherwise, compliance will be low, and the plan will have little impact. In fact, the success of the plan depends on how effective the organisation is desired (cyber) changes.

A more promising approach involves CISOs coming down from their "ivory tower" and working hand in hand with the rest of the organisation to mitigate the potential current and future impact of cyber threats on critical value chains and operations. It starts with getting buy-in right from day one. This is done by shaping the case for change as laid out in the cyber plan, explaining in lay terms what the goals are and asking the CIO and managers from the business for input and feedback. That way, solutions can be found that do the trick, but fit more easily into daily practice. The other managers will feel ownership and help create awareness in their teams. All this will result in broader acceptance and cooperation.

Cyber security has multiple **dimensions – human, process and technology** – and multiple **goals – prevention, detection and response**. The better the balance between all these in relation to the cyber risks, the more mature an organisation is or can become in cyber security terms. What counts is not only maturity, but also how consistent the security plan is implemented throughout the entire organisation. Maturity increases with organisation size, as the figures show. However, there's a significant "but". Larger multinational organisations often have to deal with increased complexity, cyber security strength can vary considerably between subsidiaries and locations. In our current hyperconnected world, ultimately, the cyber defences of an organisation are only as strong as its least protected entity or asset.

Beyond organisation-wide basic hygiene, next level maturity means that cyber security is embedded in primary processes and the overall strategy. Embedding security properly is a matter of successfully changing people's mindset as well as their ways of working. Security, by being both robust and user-friendly, is easily accepted by employees and customers alike, and as such actually contributes to better performance. This should lift organisations to an even higher level of maturity, where effortless, top-of-class security is a unique selling point that ensures customer trust.

Another way to move up the maturity curve is to **collaborate** not just internally, but also with similar organisations, supply chain partners and external experts. It's far better, in terms of effectiveness as well as efficiency, to share cyber best practices than to keep reinventing the wheel in the isolation of your own organisation. Recycling best practice cyber security solutions is often very well possible, as it doesn't involve sensitive business intelligence. So even keen competitors can work together to make their sector safer as a whole."

A cornerstone of effective organisation of cyber security is a good strategy. One that is linked to the organisation's overall strategy and to its digital strategy. In other words, a framework and plan of action designed to improve the organisation's cyber security and resilience. In this chapter we describe what progress organisations have made towards such a strategy.

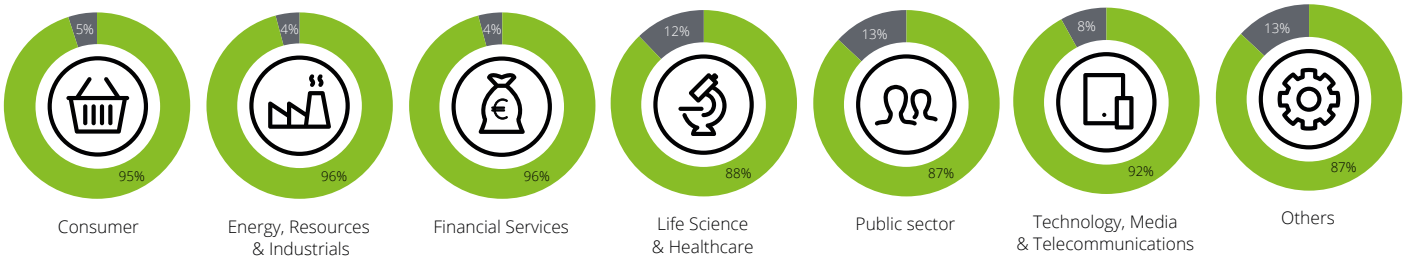
2.1 The status quo of the cyber security strategy

The fundamentals of an organisation's cyber security strategy should enable them to elevate their overall security, resulting in the protection of services and products. Such a strategy includes a plan of action designed to improve the organisation's cyber security and its overall resilience. With this in mind, our survey shows that the majority of organisations claim to have an up-to-date cyber security strategy in place. The likelihood of a cyber security strategy being in place seems to depend on the size of an organisation, notably, relatively smaller organisations either have no cyber security strategy in place or one that is not up to date.

In order to support the prioritisation of their cyber security strategy, organisations can choose to embed their cyber strategy into and align it with their organisation-wide strategy, or they can keep it information technology oriented, or they can tailor it to a specific market. Our survey shows that the larger an organisation becomes, the more often an organisation-wide cyber security strategy is in place, compared to relatively smaller organisations where we see a mix of all the above-mentioned approaches.

Does the organisation have an up-to-date cyber security strategy?

By industry

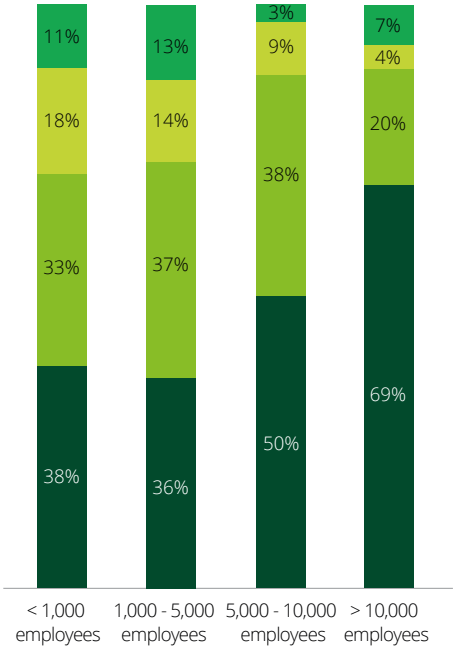


By organisation size

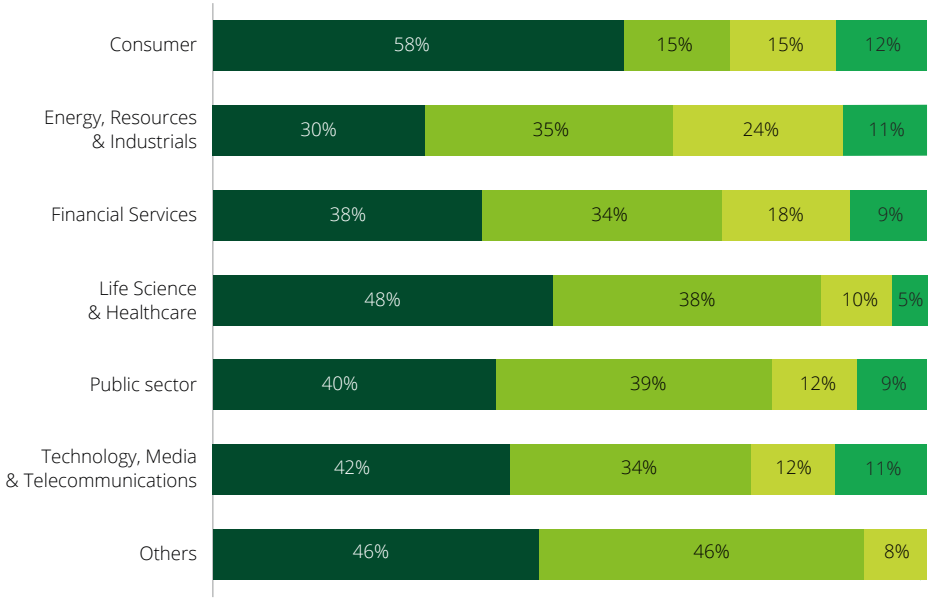
Yes
No

On which level is a cyber strategy in place?

By organisation size



By industry

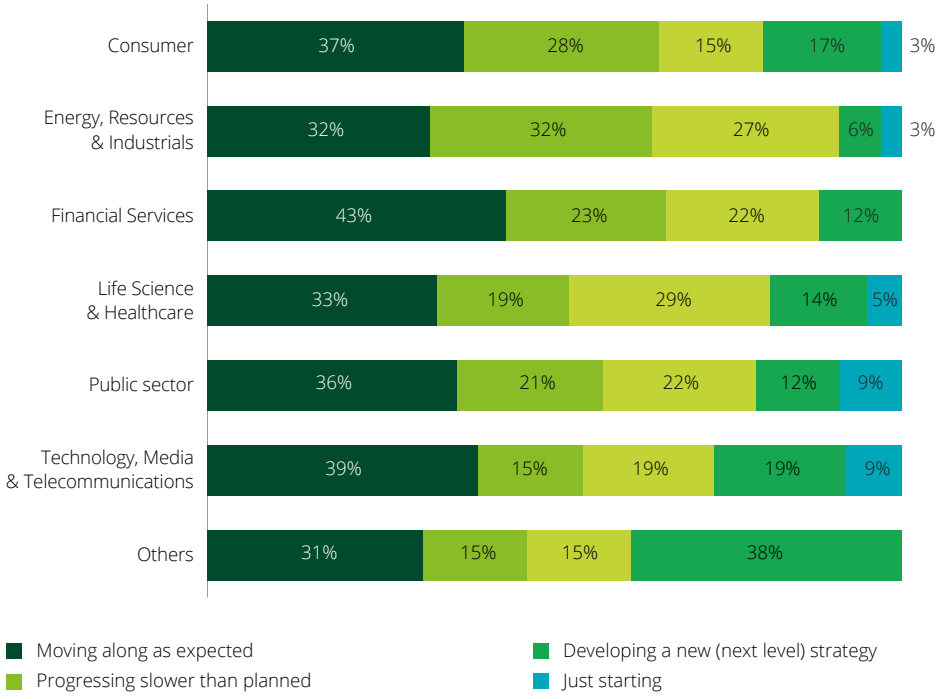


However, a cross-industry close-up reveals stagnation in the implementation of cyber strategies, as 22% of organisations are progressing slower than expected and 4% are just starting. This could indicate a disconnect between prioritisation of cyber security as a topic and the inhouse capabilities and resources to implement necessary cyber security measures.

To excel in cyber security, organisations need to dedicate resources and invest in expertise. Understandably, it is not core business for every organisation, given that 45% of our respondents said that it is challenging to dedicate enough financial resources to protect all assets. This leads to tough decisions, even in industries considered to have a mature cyber security environment.

Which statement best describes the progress of implementing the cyber strategy within your organisation?

By industry

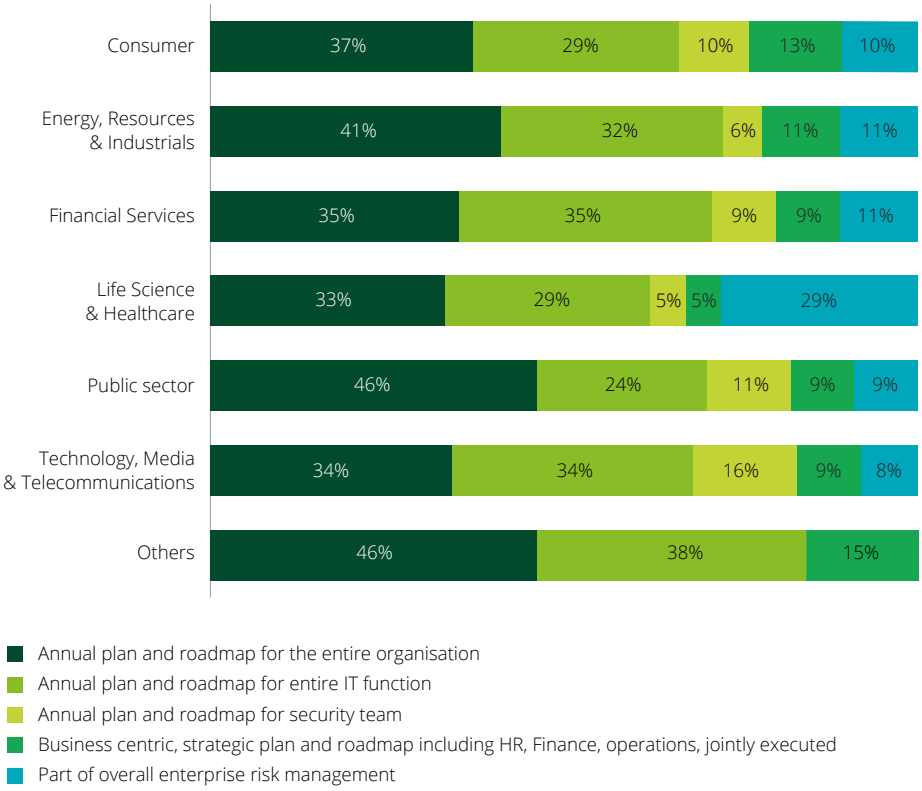


An annual plan and roadmap can help an organisation to elevate their overall security, resulting in the protection of services and products. Zooming in on an industry view regarding the characterisation of a cyber security strategy, our survey shows that:

- The **Public sector** and **ER&I** industries have the highest focus on an annual cyber strategy plan with a roadmap for the entire organisation.
- **Technology, Media & Telecommunications** and **Financial services** equally favour annual plans for the entire organisation and the entire IT function.
- Notably, 29% of the respondents from Life Sciences & Healthcare characterise their cyber strategy as part of the overall enterprise risk management framework, the highest among all the industries.

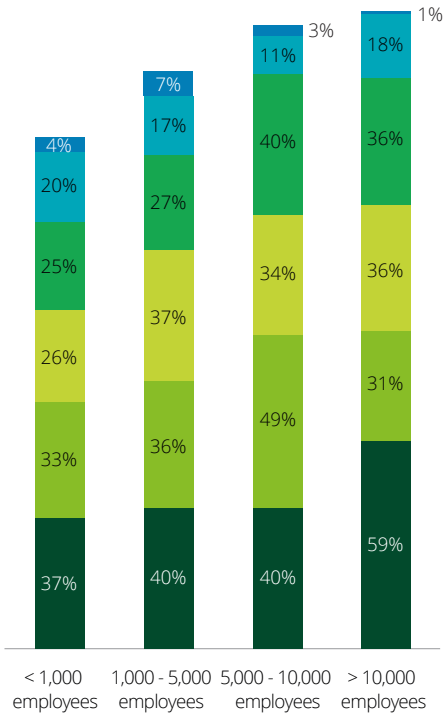
Level of cyber security strategy

By industry



Which trends do you see in your security organisation?

By organisation size



2.2 The success of cyber security strategies

Trends in the cyber security organisation

The main trends that make respondents optimistic are on the one hand growing maturity of their cyber security organisation (46% of respondents), and on the other hand stronger alignment with the business (39% of respondents). Growing maturity in the cyber security organisation is particularly highlighted by the larger organisations (59% of organisations with more than 10,000 employees).

Other trends reflecting the growing success of cyber security strategies include integration of cyber security in business teams (DevOps), innovation, improving compliance and an improved IT workforce.

Areas for attention

The survey has revealed problems which in our view require attention, given the rapidly changing cyber environment. These may derive from internal or external mechanisms.

- 60% or our respondents feel that the cyber security maturity of third parties is increasingly difficult to manage. Specifically, for organisations in the Life Sciences & Healthcare sector, 68% believes this is the case.
- 48% or our respondents feel that new technologies like quantum computing and artificial intelligence make it difficult to defend the organisation against future threats.
- 43% or our respondents say it is becoming difficult and costly to secure their environment in a way that ensures their organisation is less targeted than others. This is perceived as less of a challenge within the Life Sciences & Healthcare sector (27%), as their business model inherently requires adherence to more stringent laws and regulations due to the fact that these organisations process sensitive data of patients.
- The development of the IT workforce, in terms of attracting talent and achieving more diversity, remains a concern. On average only 17% of the respondents seem to be satisfied with trends in the IT workforce.

Success factors in achieving cyber security goals

Achieving cyber security goals, according to respondents, depends primarily on compliance with industry and market standards. Organisations are aware of external threats, but a trend is seen in protecting oneself from possible internal threats. One solution which could contribute to limiting internal threats is the implementation of Identity and Access Management (IAM) processes and technology. 46% of large organisations express that this is a critical mechanism to achieve their cyber security goals.

Our surveyed CISOs (59%) agree that the following key success factors contribute significantly towards achieving cyber security goals: monitoring, incident and vulnerability management, third party cyber risk management, supply chain risk management, disaster recovery and business continuity.

Cross industry, the majority consider compliance with industry standards (including privacy) to be among the most important factors to achieve their cyber security goals. Second and third in line are operational and communication & training activities. These three areas combined are considered to be the most critical success factors to achieve cyber security goals.

An explanation for this could be the importance of preventing reputational and financial damage when a data breach occurs or when the organisation is found out not to be compliant.

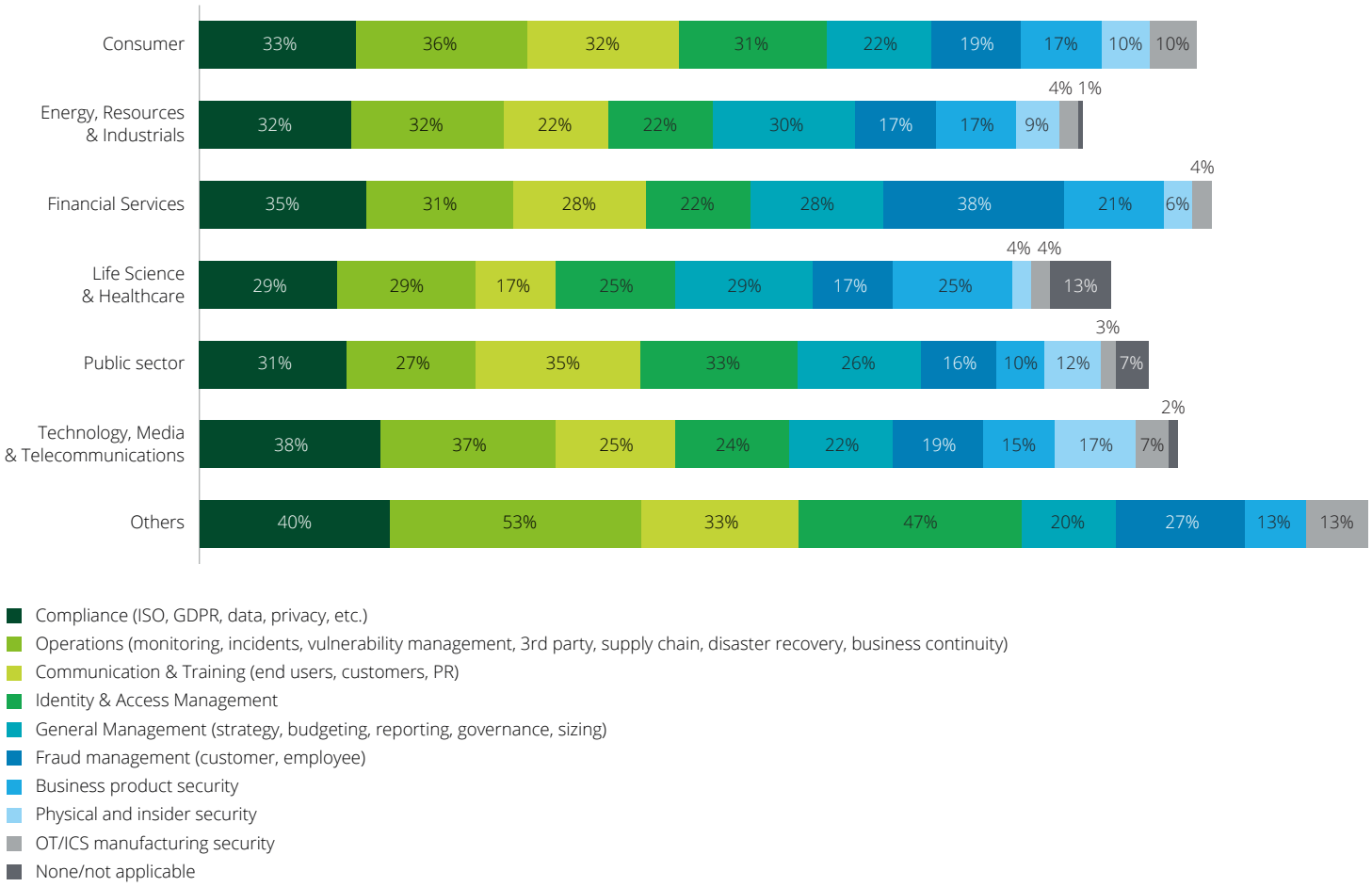
Having a cyber plan and strategy is one aspect, but making sure the implementation of the plan results in a structural cyber change is what really counts.

Key takeaways to consider are:

- To achieve a structural cyber change in your organisation, it's a good idea to explicitly plan for the anticipated change as part of your cyber strategy.
- Besides goals to increase the cyber maturity of an organisation, the cyber change efforts should be aimed at people: increasing a (cyber) risk aware mindset, embedding cyber as part of normal working routines, and nurturing a culture of informed and responsible risk taking.
- Cyber risk needs to be seen as an enterprise wide topic that matters, and is not only the responsibility of the CISO. Early buy-in of relevant leaders in an organisation is crucial for an effective implementation of a cyber plan or strategy.
- Having an understandable case for change alongside the cyber plan or strategy, as well as a clear business case and resource plan, helps to focus efforts to increase cyber maturity and will more likely result in efficient and effective realisation of cyber capabilities.

Which of the following will be the success factor(s) in achieving the cyber security goals?

By industry



Privacy and cyber security efforts strengthen each other

A Deloitte perspective by Annika Sponselee

Annika, partner Deloitte Risk Advisory and head of Deloitte Privacy & Digital Ethics Practice, has more than 15 years of experience advising clients on the legal, technical and organisational aspects of privacy.

"Some one-third of respondents perceive compliance as the most important factor for successfully achieving their cyber security goals. And they're right: compliance is important when it comes to privacy. However, my hope is that in the coming years, more organisations realise that privacy goes deeper than just compliance. In many organisations, privacy is often still seen as a showstopper. In reality, privacy in 2021 should be a business enabler. It is something that concerns consumers, making it a unique selling point.

I'm glad to see some organisations are already shifting towards handling personal data responsibly and ethically — not simply because of rules and legislation, but because of the opportunities that doing so presents. They have privacy by design as a starting point. One of our clients, a multinational company in consumer goods, has lawyers and marketeers working closely together, meaning it can cover a campaign's legal aspects at an early stage. Some banks are communicating with their clients about data considerations, giving them control over their data and, by extension, gaining their trust.

If an organisation properly and responsibly handles data, then consumer trust grows, adding significant value beyond simple compliance. When consumers know their personal data is kept safe and is not irresponsibly shared with others, they are more willing to share their information.

If consumer trust cannot be achieved, or if that trust breaks down, it is very difficult to regain. A data breach or the misuse of data, for example, can negate trust and damage brand reputation. This is why it is so important to handle data carefully. The organisations that maintain a consumer-centric approach know what consumers want from them: to stick to the rules and come up with unique strategies for creating consumer trust. Responsible data use is the future, where organisations also have their own moral compass. They must move beyond laws and regulations and ask themselves important questions: What do we, as an organisation, want to do with the data we collect? How do we ensure that we deal with that data responsibly? How do we handle technology responsibly? How do we make sure that we move beyond regulations and follow our own moral compass? Trust comes when an organisation proves it can manage and use data ethically and that it is looking beyond the law.

Privacy and cyber security should not be viewed as separate issues. The more privacy-sensitive the data is that an organisation handles, the more urgent cyber security is. Measures to better protect privacy strengthen cyber security, and stricter cyber security measures also strengthen privacy. As trust is so vital to a data-driven organisation, protecting confidential data, and thus privacy, is a top priority. Its encouraging to see, therefore, that as organisations mature, cyber security is increasingly being addressed at board level, and the cyber security strategy is becoming more integrated into the overall strategy."

3. A recipe for CISO success

A recipe for CISO success

A Deloitte perspective by Martijn Knuiman and Esther Schagen-van Luit

Martijn, partner Deloitte Cyber Risk Services, has been a cyber security advisor with Deloitte for 16 years. He now leads the Cyber Risk Vigilant & Resilient team.

"At Deloitte we organise CISO Transition and Onboarding Labs, and in my experience the issues CISOs struggle with are mostly business oriented, and far from technical: they have to do with **time, talent and relationships**. The survey results confirm that. It's no surprise that CISOs are often distracted by firefighting the latest internal issues, while they also need to keep up with the latest external threats. Meanwhile, their organisation is constantly changing. They have a role to play in major transformations, but sometimes get called in too late. Amid all this, they need to set cyber security ambitions of their own and try to make progress towards them. In our labs, CISOs learn to divide their time across issues based on urgency and importance, and to delegate.

Many respondents highlight **emerging technologies** as a challenge. There's always new malware to watch out for, and as businesses evolve, this also introduces new cyber threats. For example, manufacturers are building connectivity into their production lines to monitor and adjust processes. A fantastic innovation, but each access point could be a back door to the company's IT infrastructure. CISOs need to be involved in these projects from an early stage.

Having the right talent on the key topics reduces the challenges by at least half. It struck me that managerial and non-managerial respondents give a different ranking to the problem of "cyber risk alignment on senior stakeholder level". In other words, CISOs and other executives don't always have the same risk perception - and apparently the **CISO is the last to know**. That's a matter of communication. CISOs are good at talking to other CISOs at conferences, but explaining cyber challenges such as emerging threats in such a manner that they're easy to digest by board members is a point of improvement. Again, a non-technical and very basic challenge: **managing your relationships** and most influential stakeholders.

This touches on the role of the CISO, which is changing from being 'the department of no' to being a business advisor and enabler. For years, CISOs have had to shout to get the attention of the board, but now that they have that attention, they need to **show what their added value is** by delivering a meaningful contribution to the conversation. And to do so, they also need to listen. Successful CISOs are able to translate security technicalities into business language, making them better advisors. In our labs, we let CISOs practise doing a pitch for stakeholders in the business in 30 minutes, then 3 minutes and then 30 seconds.

Today's CISO is therefore a different personality type. A decade ago the CISO was very technically focused, whereas nowadays the CISO needs to communicate with the business and manage a diverse and inclusive team. A CISO no longer needs to rely on a deeply technical background. It's more important **to be a people person**."

Esther, Chief Information Security Officer at Deloitte Netherlands, is responsible for keeping the data of Deloitte's clients and employees secure.

"As a former consultant in the cyber team and having served many CISOs throughout my years with the firm, I thought I understood exactly what was needed from a CISO. However, stepping into the role, understanding the challenges and effectively navigating through them proved to be two very different beasts. I think my main added value is in helping our culture in IT better resemble our culture in the consulting business – in other words, we are there to serve our clients first and foremost. It's just that now the consultants, my former colleagues, are my clients. Going from the 'department of no' to the 'department of know' takes time, as we need to develop an advisory mindset. We cannot say yes to their requests if they're a mismatch with our security requirements, but we should always look for creative solutions together, solutions that still allow them to pursue their ambitions.

Having a great team in place that can deal with security operations and management autonomously, expertly and with a keen eye for the client's interests, is another priority. In return I try and enable them by automating, standardising and simplifying security where possible. Their proficiency enables me to free up time to chart a strategic course and engage my local and international stakeholders. The sheer range of stakeholders I need to interact with in order to effectively drive my security initiatives is tremendous, and as such I've made it a core priority in my role as CISO to get in touch and build relationships."

How is the role of CISOs changing? What are they struggling with? And what do they need to succeed? Respondents share their observations.

3.1 The CISO: no more "department of no"

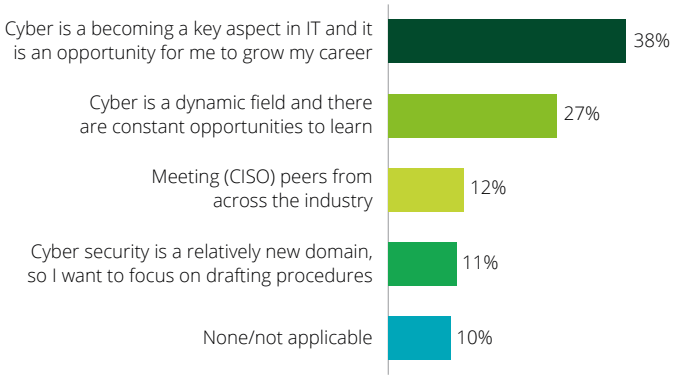
The CISO is the senior-level executive responsible for protecting information that the organisation handles. The CISO directs staff in identifying, developing, implementing and maintaining processes across the enterprise to reduce risks related to information and information technology. They respond to incidents, establish appropriate standards and controls, manage security technologies, and direct the establishment and implementation of policies and procedures. The CISO is also usually responsible for information-related compliance. According to 36% of our surveyed CISOs, the ultimate goal of cyber security is to protect people and assets from harm, misuse and abuse. And as mentioned before, the nature of their role has changed, from a purely technical to a more business integrated role, in which they operate and find solutions within their organisation while keeping an eye on emerging threats. Where in the past the CISO was considered to be the "department of no", the CISO has transitioned to a valued business advisor and an enabler for business strategy. The greatest attraction of the office of CISO (cited by 38%) lies in the rapidly growing importance of the role. This offers opportunities to have an impact on the organisation while at the same time moving up the ladder. In second place are the dynamics of the field and the constant opportunities to develop one's skills.

Who does the CISO resport to?

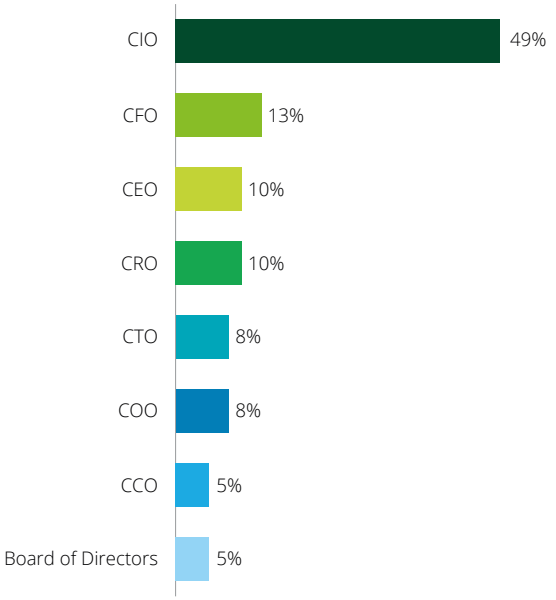
The evolution of the CISO is not limited to the subject matter. Their position within organisations has also undergone changes. In the past CISOs often reported solely to the CIO, a role that has started to shift to a board-level executive. This gave the CISO a sponsor who can influence the executive board members. In our survey 49% of the CISOs working in organisations with more than 1,000 employees directly report to the CIO. The shift can be seen in the other 51%, where 15% report directly to the CEO and/or the Board of Directors, 13% to the CFO and the remaining 28% to the CRO, CTO, COO or CCO.

The reporting line shift could be an indication of more effective and direct communication with the board, as a direct line has been established. Similarities among perspectives can be found, as 36% of CEOs and CISOs felt most strongly about setting the right security ambition in the context of the organisation's goals in order to be successful.

A CISO's personal priority



Who does the CISO typically report to in your organisation?



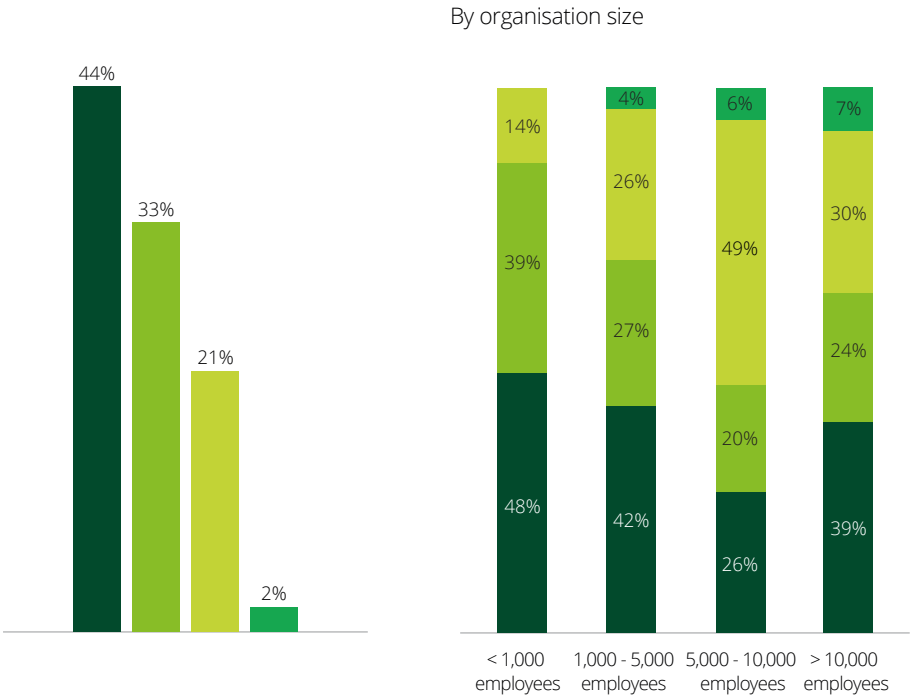
What mandate does the CISO have?
As the evolution of their role sets in, the mandate of CISOs has been adjusted. Almost half (44%) of the CISOs have a mandate to prioritise and fix problems as they see fit. This gives them the opportunity to advocate for security solutions that fix or flag cyber threats that are not on the agenda of other board-level executives.

A third (33%) of all CISOs have access to the decision-making process in the organisation. This is especially true in smaller organisations with fewer than 1,000 employees (39%), while in larger organisations (1,000 or more employees) 27% or less indicate having access to such processes.

"The role of a CISO is clear today. But what that role will look like in the near future is unclear."

- a respondent

Which statement applies best to the CISO's mandate?



3.2. Main challenges CISOs face

The increased attention to cyber incidents and their aftermath has raised the priority of cyber security among high level professionals besides CISOs. After all, protecting the cyber environment means protecting an organisation's production environment and crown jewels.

Therefore, it is no surprise that 54% of organisations admit that news of major attacks is increasing the pressure on the cyber security maturity of their organisation. This is especially true for larger organisations - 66% of organisations with 5,000 to 10,000 employees and 68% of organisations with more than 10,000 employees.

What are the challenges that CISOs face?

CISOs have to balance the needs and capabilities of their organisation while keeping up with emerging technologies and threats. There are also various other challenges for a CISO to overcome, for example: finding good professionals, executive support, sufficient budget or a mandate to participate in decision-making conversations at the right level. Interestingly, our respondents indicated that they rarely have challenges resulting from changing international laws and regulations, or from data management complexities in general. This could be an indication either that our respondents have bigger challenges to tackle at this stage, or that these upcoming challenges are well under control. Our assumption is that it is not the latter.

"We see that more and more international laws and regulations demand that data is properly protected and properly managed. It's also fair to say that this is an emerging field: not so many laws that demand proper data protection and data management are on the books so far, however many more are being proposed right now. So this could be an indication that while currently respondents indicate that they rarely have challenges on this topic, this might change in the near future."

- Jan-Jan Lowijs, Director Deloitte Cyber Risk Services

The most cited challenge faced by organisations and CISOs when it comes to managing cyber security is the overload of priorities that need to be managed simultaneously, 31% of CISOs (1,000+ employees) agree with this compared to 21% of the general population.

A cross-industry perspective shows that Financial Services, Technology, Media & Telecommunications, and Energy, Resources and Industrials face challenges with emerging technologies hindering their execution and implementation. Public Sector and Consumer industries struggle with handling too many priorities within the organisation that need to be managed simultaneously.

What gives you headaches in executing your role?

3.3 CISO success: what are the ingredients?

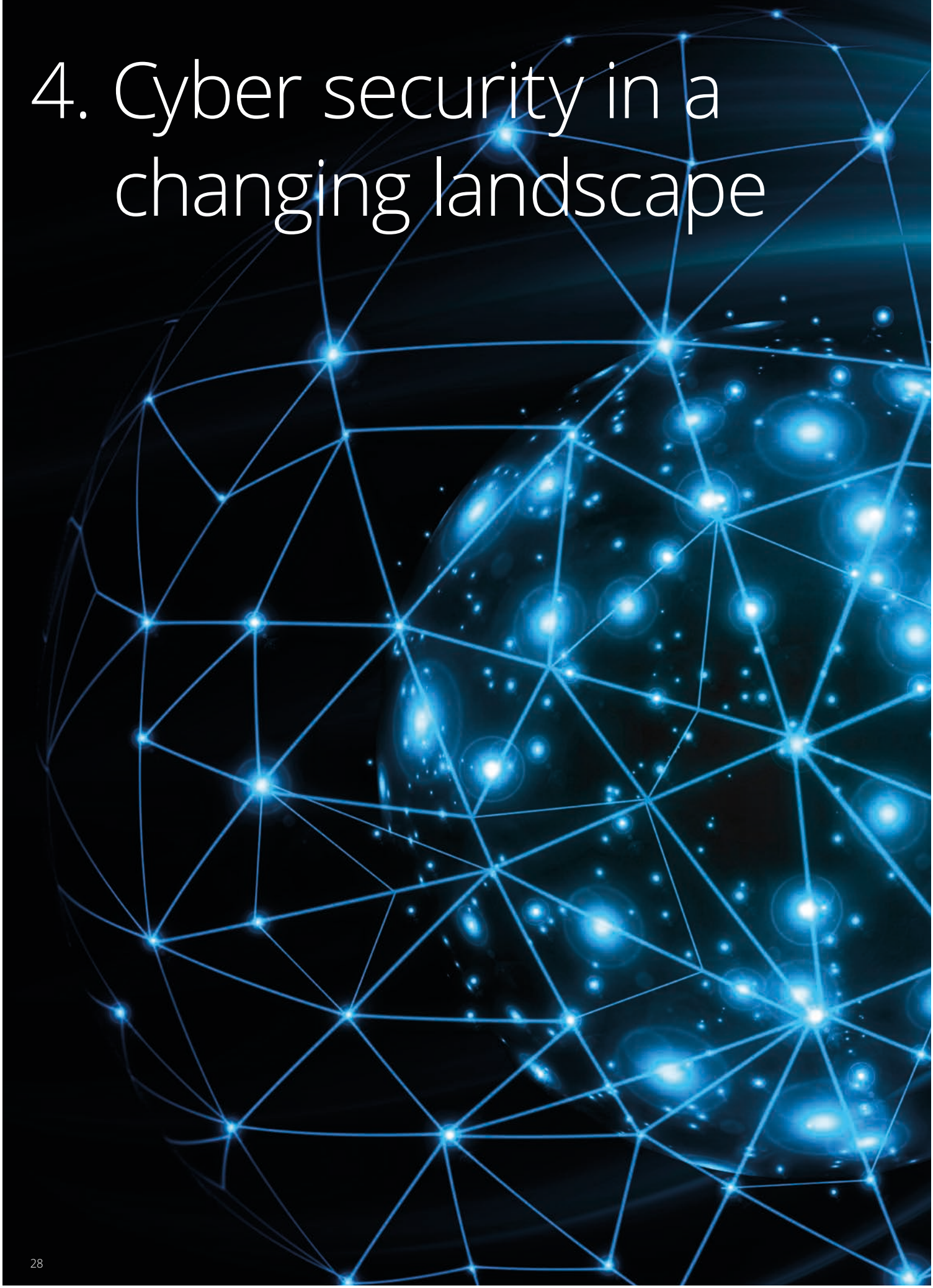
To be successful, according to respondents, a CISO needs to be a jack of all trades. Above all, they must have the talent to align the constantly changing priorities of business and IT. Meanwhile, the cyber security ambition also needs to be set and kept up-to-date at the right level, as discussed in the second chapter, where we surveyed the success factors in achieving cyber security goals. The CISO has to attract team members that are capable and equipped with knowledge fit to face organisational cyber challenges. Besides, the CISO must be good at handling budgets and investments. The diversity of desired skills is particularly notable. In short: a good CISO must above all be a good — all-round — manager.

54% of CISOs are of the opinion that setting the right security ambition in the context of their organisation's goals — in other words, defininig when good is good enough — is paramount to succeeding in their role. Other success factors mentioned are (36%) activating business/IT stakeholders to act on their respective security responsibilities and configuring the security organisation in order to effectively build and deliver the right security capabilities.

In this area there are few differences between sectors, except in the case of Life Sciences & Healthcare, where 38% believe it is even more important to align the changing priorities of business and IT.

What do you need to be successful in your role?

4. Cyber security in a changing landscape



Cyber security in a changing landscape
A Deloitte perspective by Frank Groenewegen

Frank, partner Deloitte Cyber Risk Services, has over 15 years of experience in the field of cyber. From a position of Chief Security Expert at his previous employer he recently joined Deloitte. He is a well-known media presence, who is frequently invited to discuss various cyber security topics.

"The ranking of cyber threats that respondents give is different from what I would choose. In my list, the number one digital threat to protect against is a ransomware attack, with criminals stealing and encrypting data and demanding huge ransoms to restore. Our survey shows that 40% of our respondents state that 'data leakage' is their number 1 digital threat. Attacks like this pose an immediate threat to your business continuity. Second on my list is an attack from a nation state, Spies today are not only breaking into government entities to steal classified information. They also attack corporates to steal confidential (customer) data, steal intellectual property or even destroy their network and bring their business to a halt.

I share the worries that 50% of surveyed organisations have with respect to managing cyber risks introduced by third parties. The SolarWinds incident has hopefully opened eyes once again and brought the whole third-party risk discussion back on the table. It's a good idea to offer suppliers help in improving their cyber security, but it's impossible to fully control what's happening outside your own organisation. A zero-trust approach remains best if that's possible, besides having mature detect and respond capabilities.

Respondents are right in perceiving increasing proliferation of threats. Criminals can earn far more with hacking in cyber space than burgling homes and businesses in the physical world – and the risk of getting caught is far lower. But I don't believe digital threats are becoming more sophisticated overall. Some attacks are very clever and sophisticated, and I enjoy analysing and responding to them. In most cases, though, there's no need for sophistication, since easy hacks are still effective and lucrative.

In my view, it's organisations themselves that are becoming more complex. They create, change and upgrade their infrastructure repeatedly with new systems, interconnections and patches. Meanwhile, they lack a clear overview of which systems they have, what their patch level is, or which accounts have access to what data. Attackers only need to find one vulnerability or mistake to gain access, and in a labyrinth like this, it's not hard to find one. Once a hack takes place, the time it takes for organisations to detect it is still too long. In recent cases the victims had no idea until they were tipped by a cyber security company or a law enforcement agency.

So rather than prepare for future threats like quantum computing, organisations would do well focus on the basics first. And organise regular cyber 'fire drills', with ethical hackers, not to only keep staff aware but also to test and improve their digital resilience.

Even when the basics are mature for the risk profile and risk appetite that an organisation has defined, sooner or later every organisation will experience a cyber security breach. So, it's also smart to think about your response. My advice is not to dwell on reputational fears but to share information and lessons learned. The sooner society knows about a cyber threat, the easier it is to eliminate. The aviation industry sets a great example in this respect: after a crash or near-crash, all the information is immediately shared, and an independent institution investigates. That's the mindset that will make cyber space a safer place."

This chapter focuses on the results from our survey regarding anticipated developments in cyber security, (potential) cyber threats and the organisation's confidence in handling them.

4.1 Envisioned cyber security developments

Cyber security attracts loads of attention, not only from the media, but also from internal and external stakeholders. Meanwhile, the cat-and-mouse-game continues between on the one hand cyber developments within organisations and on the other hand the evolving cyber threats.

Possibly due to this constant pursuit, 26% of the CISOs of organisations with more than 1,000 employees see the increasing importance of employee awareness, training and behaviour as a key anticipated development in cyber security. There is an upward trend in this perception among the IT professionals that were surveyed when compared to the size of their organisation, with 34% of respondents from an organisation with 5,000 - 10,000 employees and 40% of respondents from an organisation with more than 10,000 employees marking this development as key. These numbers are significantly higher when compared to respondents from smaller organisations, as can be seen in the following graph.

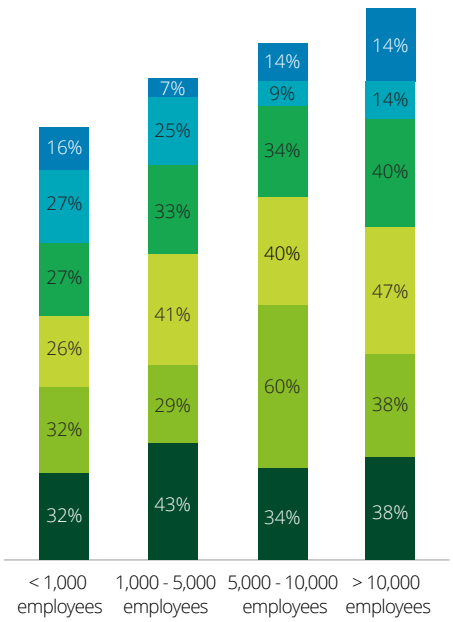
The envisioned cyber security developments can also be analysed based on industry, as highlighted in the next graph. The results from our survey show that the increasing importance of employee awareness, training and behaviour is the most anticipated development within the Public Sector; with 44% of our respondents from the Public Sector marking this as such. This same perception is also witnessed in the Life Science & Healthcare industry (42%). One might ask whether this has something to do with the employees' responsibilities and/or handling of particular data.

"For us, the most valuable development of the past year was managed detection and response."

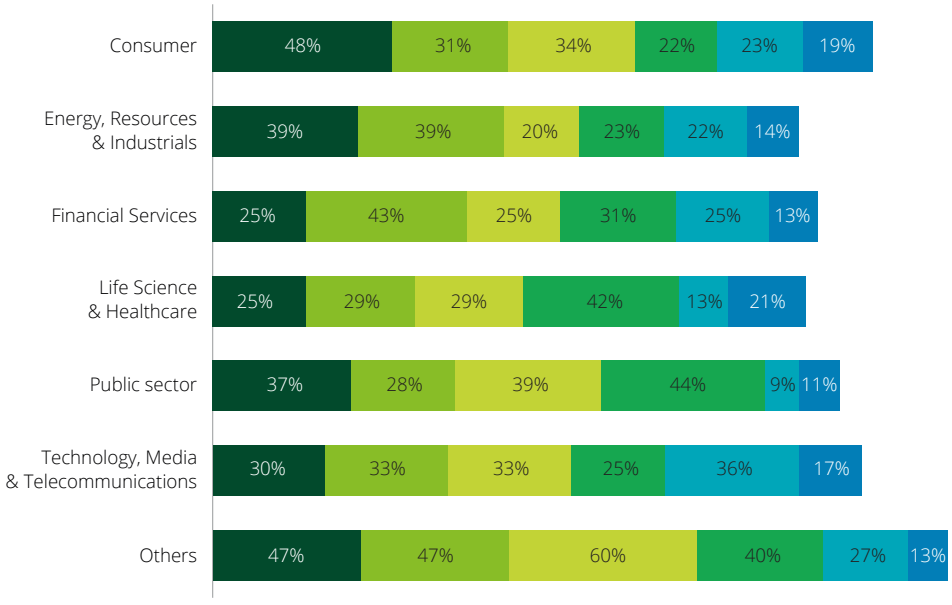
- a respondent

What developments do you anticipate?

By organisation size



By industry



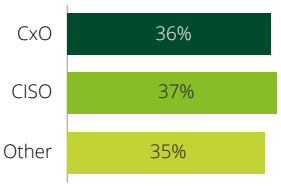
- Increasing sophistication and proliferation of threats
- Increased importance of identity and access management
- Increasing utilisation of cloud technology
- Increasing importance of employee awareness, training and behaviour
- Separation of IT and OT automation and security
- Increased importance of OT security

4.2 Threat perceptions

When regarding the previous two graphs on anticipated cyber security developments, there is one category among the answers that is fairly out of an organisation's control. Our survey shows that 36% of the CxOs foresee an increasing sophistication and proliferation of threats in the upcoming future as key development in cyber security.

Threat perceptions

By role



There is significant agreement on this vision, with 67% of CISOs (>1,000 employees) deeming this evolution of threats to be the key development that organisations need to be aware of in order to anticipate and to be resilient.

When taking a closer look at the industries, we see a similar pattern. For example, most of the respondents (48%) mention that increasing sophistication and proliferation of threats is their foremost anticipated development in cyber security. Also the respondents from the Energy, Resources & Industrials acknowledge this (39%)

However, as Frank Groenewegen stated, threats posed by organisational complexity should not be underestimated. The fact that organisations' lack a clear understanding of their infrastructural environment and, for example, packing of patch management gives threat actors relatively easy entrance into the organisation's systems. The starting point to improve an organisation's cyber security and resilience is improving basic internal security processes.

In our survey, we asked the respondents to what extent they agree with several statements about cyber security. The results are visualised in the following graphs.

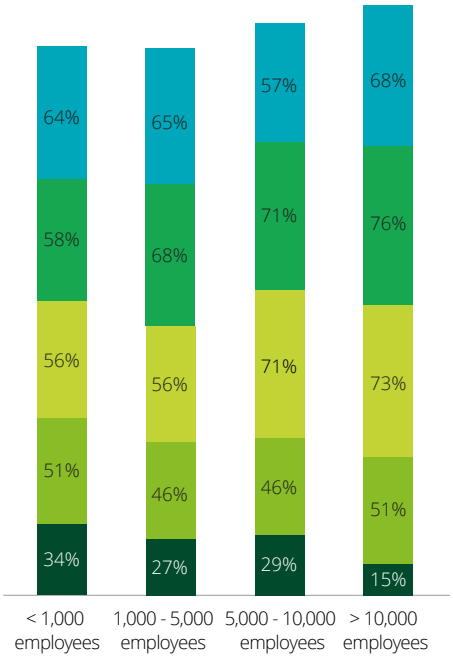
"I don't believe digital threats are becoming more sophisticated overall. (...) In most cases, though, there's no need for sophistication, since easy hacks are still effective and lucrative."

- Frank Groenewegen

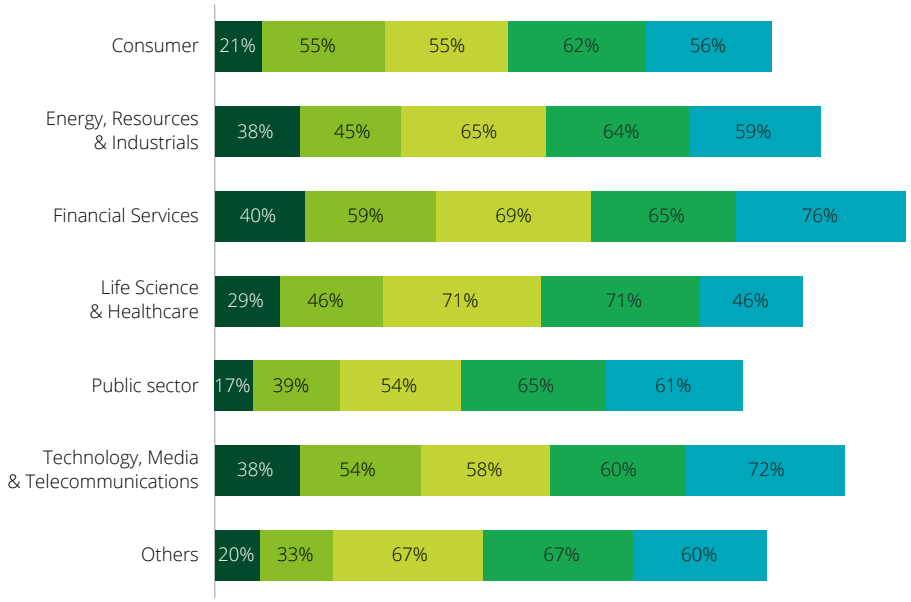
To what extent do you agree with the following statements about cyber security?

- In case of a ransomware attack, I would certainly pay to get my data back
- I'm getting more concerned about security maturity of the third parties my organisation digitally collaborates with than our own resiliency
- The security maturity of third parties is increasingly difficult to manage
- The attack surface of all organisations is rapidly increasing
- I'm confident that my organisation has built up enough stamina and fortitude to stand up after an attack

By organisation size



By industry



As can be seen in the previous graphs, in addition to the discussed evolving threats, many respondents of our survey believe the attack surface of organisations is rapidly increasing. Between 60% and 71% of our respondents from several industries mention this.

The belief in rapidly increasing attack surfaces particularly resonates within the larger organisations:

- 71% of IT professionals within organisations of 5,000 - 10,000 employees state this.
- 76% of IT professionals within organisations of more than 10,000 employees state this.

The results show an ascending trend in this regard; the bigger the organisation, the higher the percentage of respondents who believe in this rapidly increasing attack surface. However, among the CxO respondents, 83% agreed with the statement that the attack surface of all organisations is rapidly increasing. One might assume that bigger organisations have a larger attack surface, but there might also be a lurking lack of awareness within smaller organisations.

As mentioned by Frank Groenewegen in the introduction of this chapter, a particular threat that is becoming more widespread these past few years is ransomware. We have asked the respondents of our survey whether they would certainly pay the ransom in order to get their data back in the case of a ransomware attack. There is a descending trend in the results from our survey when regarding the size of the organisation (results can also be seen in the previous graphs):

- 34% of IT professionals within smaller organisations (<1,000 employees) agree with this statement.
- 27-29% of IT professionals within organisations of 1,000 - 10,000 employees agree with this statement;
- 15% of IT professionals within organisations of more than 10,000 employees agree with this statement.

It is a positive development that organisations are becoming less willing to pay criminals to get their data back, as this could imply that organisations are incorporating solutions to restore their own data and become more resilient towards ransomware attacks.

In addition to these numbers, the vast majority of CxO respondents disagreed with this statement; 61% said “no” to certainly paying the ransom to get the data back. When regarding industries, IT professionals within Public Sector, Consumer, Life Science & Healthcare, and Other are least likely to pay in the case of a ransomware attack.

“We don’t know which next-gen threats we will be up against, neither do we know which next-gen opportunities we will get to protect ourselves.”

- a respondent

4.3 Concerns with managing third party cyber risks

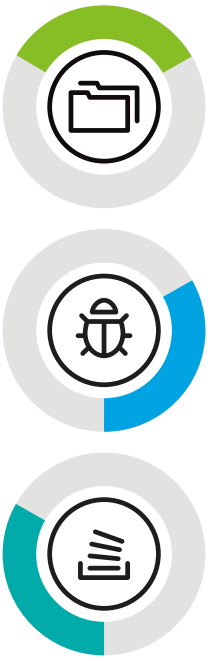
As mentioned by Frank Groenewegen earlier in this chapter, numerous organisations are dealing with concerns regarding third parties which could impact resilience. As can be seen in the graphs in the previous paragraph, 51% of respondents from large organisations (10,000+ employees) say that they are getting more concerned about the security maturity of the third parties their organisation digitally collaborates with. Financial Services organisations resonate most with this statement; 59% of respondents from this industry made the same remark. In addition to these concerns, 73% of respondents from large organisations (10,000+ employees) state that the security maturity of third parties is increasingly difficult to manage.

61% of our respondents express more concerns about the security maturity of third parties than about their own resilience against cyber threats. A remarkable 72% of CISO respondents with 1,000+ employees feel that the security maturity of third parties is increasingly difficult to manage. A large number of organisations participated in this study, of which many might be part of each other's supply chain. With all this in mind, 59% of CISOs with 1,000+ employees nevertheless feel that they are resilient against cyber threats, which might indicate a trust gap in the supply chain.

Other threats that can keep us up at night

Beside third-party concerns, the following graphs illustrate that there are other threats that can keep IT professionals up at night. Respondents from bigger organisations (1,000-10,000+) mentioned the same top three of threats:

Top three threats:



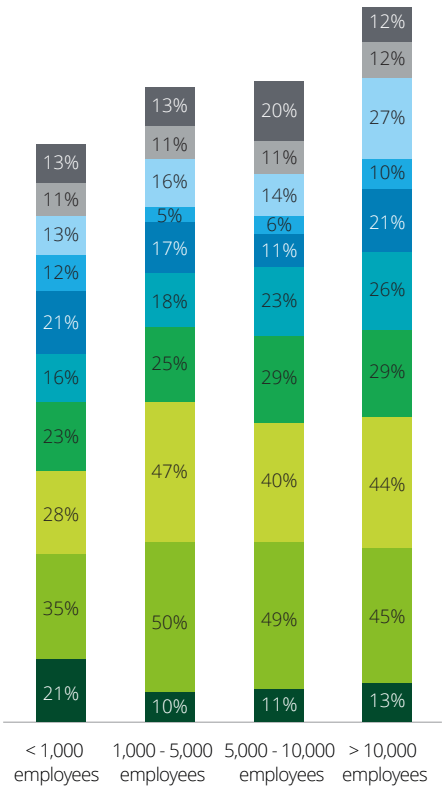
Data leakage

Phishing, malware, or vulnerability exploits

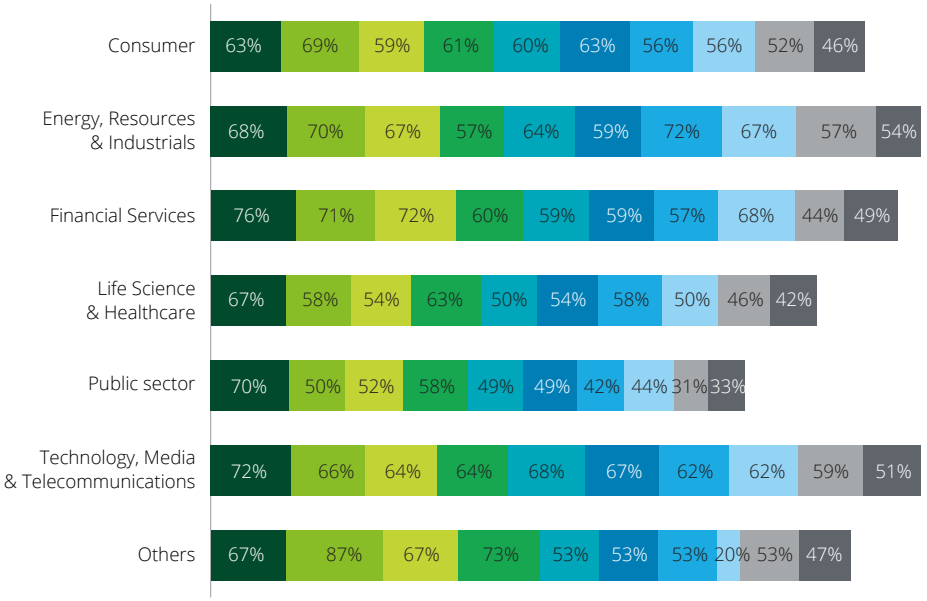
Extortion or destruction of the organisation's data

Feared cyber threats

By organisation size



By industry



- COVID-19 impact on prioritising cyber investments
- Data leakage
- Phishing, malware, or vulnerability exploits, making us an easy target
- Extortion or destruction of the organisation's data
- Employee abuse of IT systems and information
- Espionage or theft of our IP or financial assets
- Differing cultural interpretations of security positive behaviour (millennials, lax behaviour)
- Security breaches involving third-party organisations
- Supply chain attacks
- Zero days attacks

Confidently responding to threats

In the previous section, we identified the top three threats that keep people awake at night. Interestingly, respondents also indicated that they feel confident they can handle these threats.

It is also interesting to note that all IT professionals, no matter the size of the organisation, have the biggest confidence in handling the impact of COVID-19 on prioritising cyber investments. This confidence seems to grow with the size of the organisation; from 74% of respondents from organisations with 1,000-5,000 employees to 85% of respondents from organisations with over 10,000 employees. Nevertheless, this leaves the question what the actual prioritisation or resource allocation for cyber investments will be, particularly during the prevalence of COVID-19.

Confidence in handling other threats is more varied across organisation size. Interestingly, IT professionals from companies with 1,000-5,000 employees and IT professionals from companies with over 10,000 employees have the most confidence in handling the same top three threats that were just mentioned as the most severe:

Data leakage

Phishing, malware, or vulnerability exploits

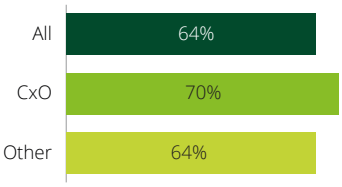
Extortion or destruction of the organisation's data

Respondents from companies with 5,000-10,000 employees have the most confidence in handling data leakage, differing cultural interpretations of security positive behaviour, and espionage or theft of their IP or financial assets. Results from organisations with fewer than 1,000 employees can be viewed in the corresponding graphs, along with industry-specific results.

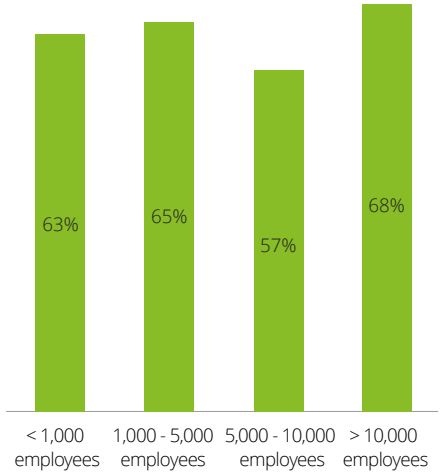
Finally, we asked our respondents whether they are confident that their organisation has built up enough stamina and fortitude to stand up after an attack. Our survey shows that 68% of IT professionals in large organisations (10,000+ employees) have confidence in this regard. This aligns with 70% of the CxO respondents that expressed the same confidence. Based on the results of our survey as discussed in this chapter, chances are that this number will rise with the envisioned increase in the importance of employee awareness, training and behaviour, especially when paired with the will to develop or opt for solutions to mitigate the risk of threats like data leakage, phishing, malware (e.g. ransomware), vulnerability exploits, or the extortion and destruction of the organisation's data.

I am confident that my organisation has built up enough stamina and fortitude to stand up after an attack

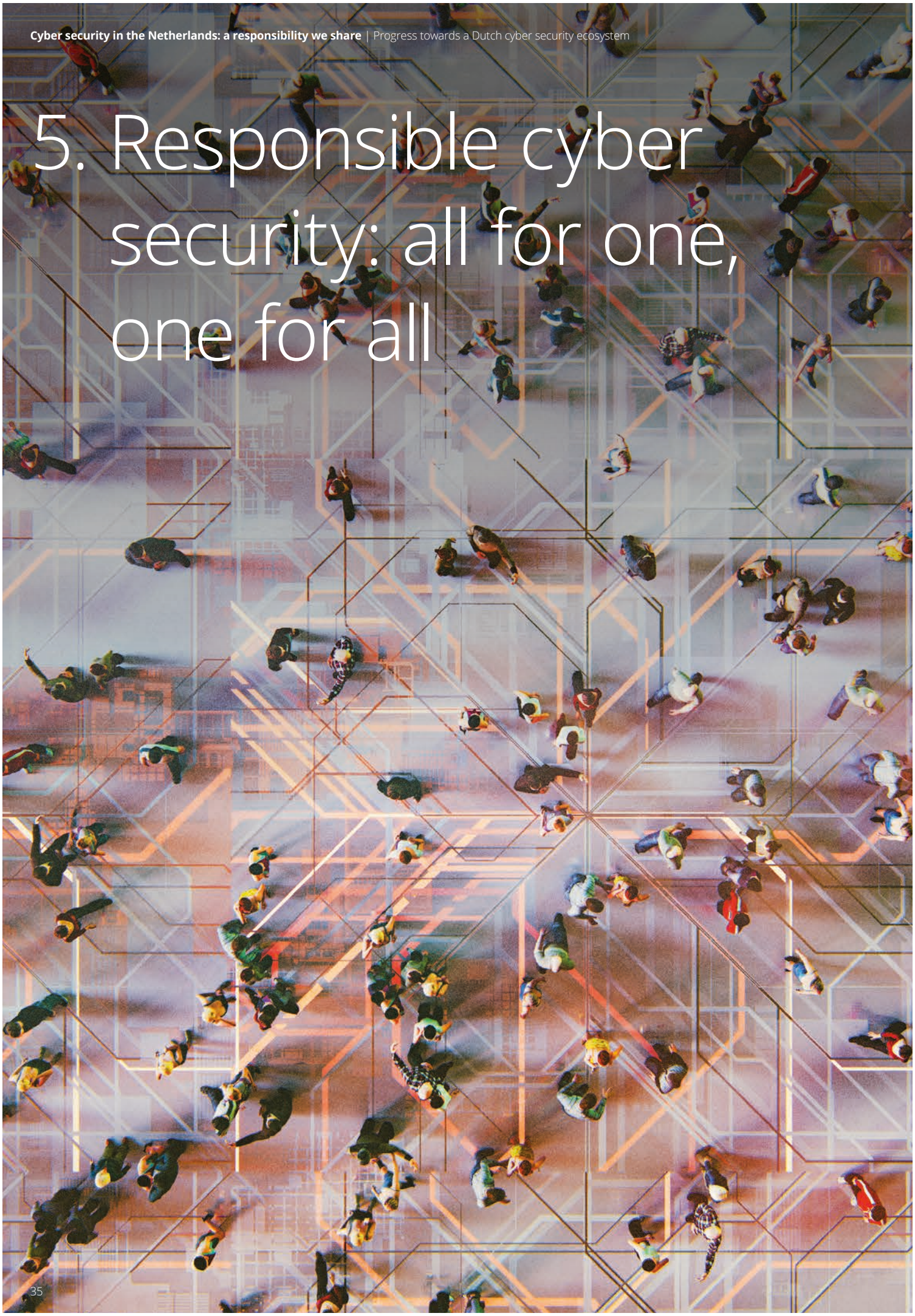
By role



By organisation size



5. Responsible cyber security: all for one, one for all



Responsible cyber security: all for one, one for all

A Deloitte perspective by Kevin Jonkers

Kevin, director Deloitte Cyber Risk Services, has worked in cyber security for almost 15 years. Besides his role as public sector lead in the Deloitte Cyber team, he is also a board member at industry association Cyberveilig Nederland. Kevin also actively contributes to public-private partnerships like Hack_Right and the Cyber Security Alliance.

"My activities in various public-private partnership initiatives really build on the broadly supported view that cyber security is a joint responsibility between organisations themselves and our government. Just as in the physical world, we are all expected to take some necessary precautions ourselves to secure our IT infrastructure. At the same time, we expect our government to play a big role in preventing, investigating, prosecuting and punishing criminal activities. Balancing and aligning responsibilities and ensuring the best possible cooperation between various stakeholders are all still very much in development. We are progressing step by step, and we quickly need to learn to walk and then run.

A key topic for discussion is sharing so-called "threat intelligence" such as information about threat actors, their modus operandi, their motivation, (potential) targets, infrastructure and the malware they use. Government institutions, private organisations and cyber security specialists are sitting on an enormous pile of such intelligence, but sharing is not happening at the scale we need for it to be effective. Currently, the Dutch government is setting up a nationwide system for sharing information on cyber threats (also known as Landelijk Dekkend Stelsel). However, work is in the start-up phase. Partly this is a matter of organisational and legal obstacles that our government needs to iron out. On the other hand, organisations have a role in this problem, too. They don't feel safe yet to share information that might be commercially sensitive or reputationally damaging. On the other hand, going it alone in cyber security carries risks, too — often bigger risks. Ideally, the nationwide system will offer organisations a safe environment where openness on cyber security related matters does not backfire.

When speaking with clients in the private sector, we tend to see that the more cyber mature organisations (often large corporates and financials) have understood that cooperation in their sectors and with governments (e.g. intelligence agencies, National Cyber Security Centres and Police) is crucial to stay on top of the threats they face. However, that's only the tip of the iceberg. Small and Medium Enterprises in the Netherlands usually don't have the time or budget to achieve the same level of maturity on their own. Since even large corporates rely heavily on smaller organisations in their supply chains, this poses a problem for our society as a whole. I already see some instances where larger organisations are trying to support their smaller suppliers or even competitors, but we need a step-up by our government as well. They can help enforce security requirements for hard- and software allowed on our markets and a default level of security that must be built into IT services. After all, would you buy a car without all the required safety features like seat belts and air bags? So why do we accept insecure IT on the market?

Overall, we are in need of a more strategic and structured approach to tackle this problem at national level. Many organisations would like to contribute, but simply don't have the right channel or means to do so yet. A national strategy can help. This could include lessons learned from sectors, like our banking sector, where various successful initiatives on sharing intelligence, broad security testing and combating fraud together have already proven valuable.

The survey shows variation according to organisation size and sector, but managerial and non-managerial respondents are remarkably in agreement. In itself this is good news, as it means that both at a strategic and an operational level, agreement can be found that cooperation between public and private is of vital importance."

This chapter focuses on the results from our survey regarding a sense of duty, shared responsibilities and contributing to a safe and secure cyber resilient society.

5.1 Doing one's duty

According to 25% of the respondents, the ultimate goal of cyber security is to protect people and assets from harm, misuse and abuse. 22% opined that protecting the vital assets of the company is the most important objective. For at least one out of ten, the ultimate goal of cyber security is making the digital ecosystem a safer place.

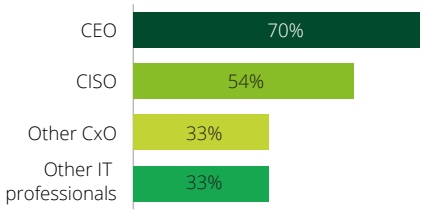
This being said, each organisation is responsible for its own cyber security. At the same time, however, they are asked to contribute to a secure Dutch cyber society. All should contribute towards a society in which it is safe to do business, live and consume electronically.

In line with this vision, we have asked our respondents whether they experience this call of duty and whether they feel responsible in ensuring that people pursuing a career in cybercrime face legal repercussions. One way for organisations to take responsibility is sharing information on (potential) attacks with other organisations and with the government by reporting the (attempted) cyber attack. A further step for the organisation is to chase and uncover the cybercriminals and actively work with the police in bringing them to justice. As the following graph shows, the vast majority of IT professionals support this view; between 65% and 71% (depending on organisation size and industry) of our survey's respondents agree with the statement that an organisation has such a duty of care and must ensure that cyber criminals are criminally prosecuted. CISOs are in even stronger agreement; 74% feel responsible in this regard.

Besides actively responding to cybercrime, detection and prevention are responsibilities that organisations are encouraged to take. However, as can be seen in the following graph, some respondents of our survey state that effectively preventing cybercrime comes at the expense of privacy. 70% of IT professionals that are in the role of CEO (or equivalent) and 54% that are in the role of CISO (or equivalent) agree with this statement. This differs from the other surveyed CxOs and IT professionals; 67% said "no" to this statement.

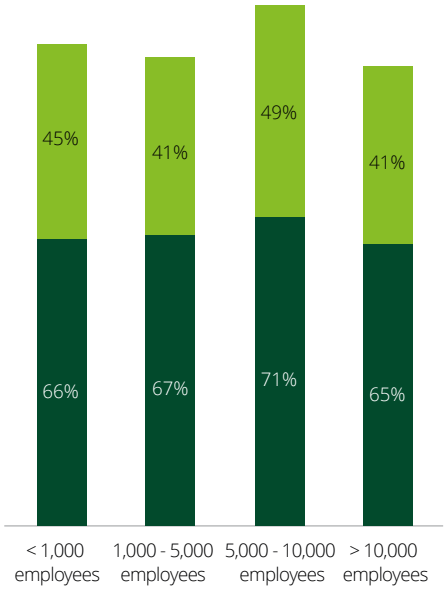
What in your opinion is the ultimate goal of cyber security?

Effectively preventing cybercrime comes at the expense of privacy (% agree)



These diverging opinions can also be witnessed when comparing the surveyed industries. It seems there might be various perceptions of the impact on privacy (and indeed of privacy itself). Moreover, it is up for debate to what extent a potential breach of privacy can be justified, for example for the greater good of sharing information and lessons learned.

To what extent do you agree with the following statements about cyber security?



"It's very interesting to see the widely diverging responses to this question. But they're not contradictory per se. On the one hand there is the realisation that preventing cybercrime would probably benefit from the ability to analyse more data – some of which will be personal data. On the other hand it is acknowledgement of the fact that when analysis is done properly, and within the boundaries set by privacy rules, preventing cybercrime does not necessarily come at the expense of individuals' privacy. Adding to that is the fact that preventing cybercrime is also beneficial for individuals' privacy, as less personal data is leaked or stolen. So the appeal to every CISO and every CxO is: if you do want to use personal data for preventing cybercrime, actively align that intended use with privacy considerations. Can we use less personal data? Can we pseudonymise or anonymise that data? Do we make sure we destroy that data as soon as possible? In other words, design your systems optimally, balancing cybercrime prevention with individuals' privacy. This needs to be full-sum, not zero-sum."

– Jan-Jan Lowijs, Director Deloitte Cyber Risk Services

"The details of security incidents and their causes are often kept secret. That makes it more difficult to learn from each other and improve security."

- a respondent

5.2 A shared responsibility

As highlighted by Kevin Jonkers in the introduction of this chapter, creating a cyber resilient society can only be effectively achieved together rather than alone. It is vital to mature cyber security throughout the organisation's supply chain. 59% of surveyed CISOs (1,000+ employees) stated that operations, including third parties, are a key success factor in achieving cyber security goals. This pairs with a perceived lack of confidence regarding how to handle supply chain attacks; respondents across all industries and organisation sizes have the least confidence in handling zero day attacks and/or supply chain attacks (as can be seen in the threat graphs in the previous chapter).

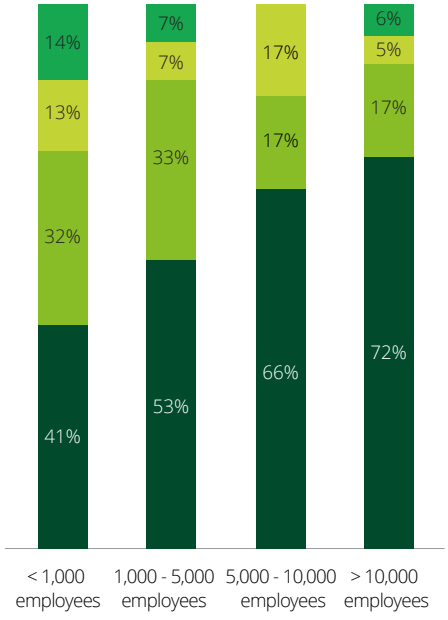
Besides corporate responsibility, many respondents from various industries commented on the governmental and societal aspects of this shared responsibility in creating a cyber resilient society. As can be seen in the graph (by organisation size), the bigger the size of the company, the stronger the belief it's the responsibility of both organisations and government(s) to achieve a cyber resilient sector. 72% of surveyed CISOs (1,000+ employees) share the opinion of the respondents working with large organisations. These results highlight the call for improved alignment and closer cooperation among all parties that play a part in our society's cyber resilience.

"What we need is fewer political restrictions to share incident information, creating more transparency. That paves the road to sharing best practices and learning from each other."

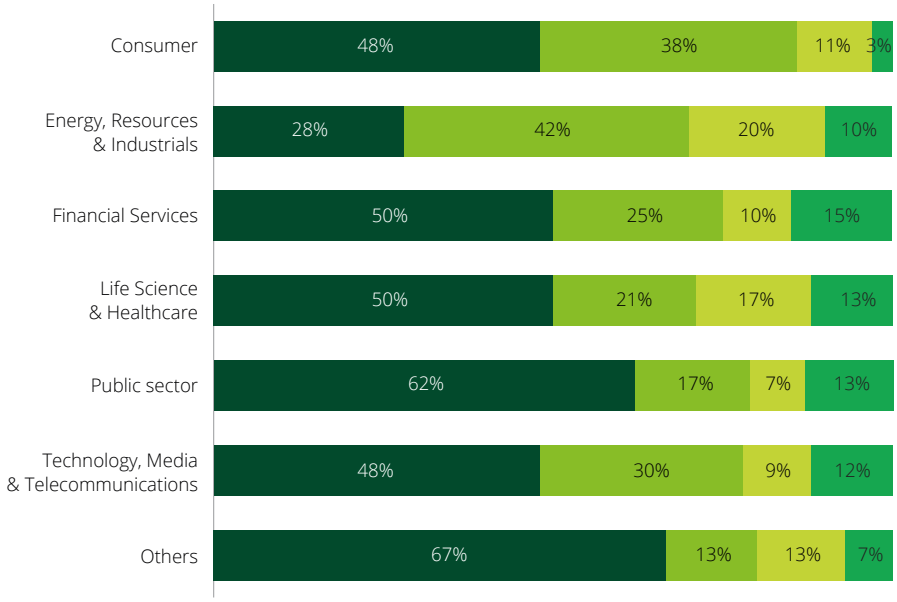
- a respondent

Who is responsible to achieve a cyber resilient sector?

By organisation size



By industry



- Companies and government
- Companies themselves
- Companies together
- Government

5.3 Contributing to a cyber resilient society

It's great how our survey shows that many organisations have a deep feeling of responsibility and actively think about what they can do to contribute to a more cyber resilient society. We asked our respondents whether they see opportunities for organisations to contribute to a more resilient sector and a cyber resilient society. The creativity, confidence and positivity in this regard seems to grow with organisation size (as can also be seen in the following graph). For example, IT professionals from large organisations (10,000+ employees) are the most positive in this regard, with 63% seeing these opportunities. The surveyed CISOs leave little room for interpretation in this regard; **100% of these respondents** see opportunities for organisations to contribute to a more cyber resilient society. These results seem to highlight the evolution towards a safer and more resilient digital society.

Do you see opportunities for companies to contribute to a more resilient sector and a safer digital ecosystem?

By organisation size

"Structural cooperation between organisations and industries is the road to a safer, cyber resilient society. Examples include sector-specific consultations or knowledge bodies, in which there is no room for mutual competition."

- several respondents

It is heartening to see such broad support, especially in the upper echelons of organisations, for more collaboration and partnership to ensure a cyber resilient society. The results underline that over the past years, stakeholders in all kinds of roles and positions have started to see that the only way to successfully combat cyber threats is by working together. This is an important step towards actually delivering on such ambitions.

The key challenge for the coming years will be to channel all this positive energy and activity in a structured and efficient way. This requires a more integrated and centralised consensus and direction, in which both public and private organisations are well represented. Let's bring down the barriers that we still face in our efforts to increase collaboration in this space, be they legal, organisational or cultural. By doing so, we can combine national and sectoral cyber resilience to build a truly cyber resilient society.

Conclusion

More than fifty years ago today, the first message was sent over the internet. Digitalisation has since then managed to impact our lives in ways that we couldn't have dreamed of at the time. It enables our societies to strive and continuously reinvent themselves. But great progress has also brought new risks. The digital infrastructure that our societies rely on has become alarmingly complex. A variety of actors pose a threat to our digital world. Security experts across industries and from organisations big and small work to keep their organisation, and our society, cyber secure. This report has provided insight into what they think and feel.

More and more organisations nowadays have at least a basic understanding of the importance of cyber security investments. Most have translated this into cyber security plans or strategies, and almost half have seen a rise of more than 6% in budget per year. This indicates that boards understand the importance of a cyber secure organisation and the necessity to invest. The many examples in the news of Dutch organisations hit by cyber attacks in the past years has likely added to this understanding.

Effectively executing cyber security initiatives is hard. Almost a quarter of the respondents are behind on their planning. What helps is engaging with the business, forming partnerships and communicating security as an enabler rather than simply a cost item. We increasingly understand that the ability of CISOs to influence the security maturity of their organisations is based on their ability to influence people.

Our respondents are often optimists. They are confident that they can handle cyber security threats, are not worried about the impact of COVID-19 on their budgets, and a large majority think their organisation can withstand a cyber attack. More than sixty percent of CISOs chose the role because they think it will become increasingly important and provides them with opportunities to learn and grow. That said, a similar number of them also feel they have too much on their plate already, while they must also keep their organisation future proof and ready for next-generation threats. Boards must understand that cyber security is a shared responsibility and that they must make joint decisions on realistic and pragmatic goals. This requires not only awareness of problems and solutions, but also commitment to make tough decisions. It's difficult to prepare for the threats of tomorrow if you're not ready for the threats of today.

Because the current threat landscape is already challenging. Just one key vulnerability is often all attackers need. The sheer size and complexity of modern organisations raises the question to what extent organisations can, and dare to, rely on their defensive capabilities. Risks also lurk in complex supply chains, in which organisations depend on each other's cyber security measures but are not able to exert significant influence over them. Organisations can go a long way in managing their risks by focusing on basic cyber security hygiene and detection mechanisms, and exercising risk-based control over suppliers. As a society, we should focus on enforcing standards that raise the expected security level to a shared minimum. Defining this level is a complex issue, given that cyber risk is just one of the many risks our society faces, and can require significantly more investment depending on our ambition.

Being cyber secure is not enough, however. Either for individual organisations or for society as a whole. To continue our digital journey with confidence, we need to be able to take a blow and stand up again. In other words, we need to become cyber resilient. Making our society more cyber resilient is a shared responsibility. The response rate of our survey is high, and most respondents see a role for themselves and their organisations in contributing to a more secure sector. This indicates that a vision of working together is shared across the Netherlands. Going forward, cyber security will only become more important, as both basic and advanced threats are on the rise. We will need to leverage each other's wisdom and support in the coming years, across academia, government and the private sector. This may mean sharing information on threats and incidents more effectively, but also exchanging ideas and lessons learned. The government needs to take a leading role in converting the energy and goodwill in the security sector into clear and effective initiatives that make the Netherlands more cyber resilient.

If we can define shared cyber security goals and work together to achieve them, we can reap the benefits of digitalisation in the Netherlands for the next fifty years and beyond. We already have our key role in global high-frequency trading on financial markets, our champion in semiconductor technology, and our world-class automated port of Rotterdam. What will be next?

Deloitte is committed to the cause of helping our clients build responsible businesses that play their part in a cyber resilient society. In order to do so, we want to help facilitate the next steps by:

- Organising round tables and sessions that bring key stakeholders on cyber resilience together to discuss concrete and meaningful actions we can take collectively
- Bringing our expertise to CISOs to help them grow in their role and accelerate their journey as leaders
- Being an active voice and contributor to the public debate around cyber resilience in the Netherlands

With a culture of understanding, connection and trust, we help create opportunity and enduring success. With cyber everywhere, it's a shared responsibility. Are you in?

About Deloitte Cyber Risk Services

The Deloitte difference

In this digital world, your reputation begins and ends with cyber. As a worldwide leader in cyber strategy consulting and cyber intelligence, Deloitte offers a fully customisable suite of cyber solutions and managed services.

With a commitment to technological innovation and broad industry expertise, our Deloitte global network gives us the insight and experience to face any scenario. Because we listen to your needs, Deloitte Cyber is uniquely equipped to help you navigate the evolving landscape for a successful and more responsible future.

Cyber capabilities

- 22,000 Cyber practitioners worldwide
- 30+ Years in providing Cyber Risk Capabilities
- Ongoing projects include Detect and respond, Identity Access Management, Strategy, Application Security, and Data and Privacy for OG&C clients
- 2000+ certified information systems security specialists globally

Accolades

- Ranked #1 globally in Security Consulting, 10 consecutive years based on revenue by Gartner[1]
- Deloitte named a leader in Managed Security Services 2020 Vendor Assessment[2]
- Deloitte named a global leader in Cybersecurity Consulting by ALM[3]

[1]Source: Gartner, Market Share: Security Consulting Services Worldwide, 2020, Elizabeth Kim, April 2021

[2]Source: IDC MarketScape: Worldwide Managed Security Services 2020 Vendor Assessment by Martha Vazquez, September 2020, IDC #US46235320e

[3]Source: ALM Intelligence; Cybersecurity Consulting 2019; ALM Intelligence estimates © 2019 ALM Media Properties, LLC. Reproduced under license

Acknowledgements and contact details

Acknowledgements

We wish to thank:

Marco Kanis
Senior manager Cyber Risk Services

Yhennifer Cornelia
Consultant Cyber Risk Services

Iris Rieff
Junior manager Cyber Risk Services

Casper Stap
Senior consultant Cyber Risk Services

Jan-Jan Lowijs
Director Cyber Risk Services

Esther Schagen-van Luit
Chief Information Security Officer
Deloitte Netherlands

Robbin van den Dobbelsteen
Director Cyber Risk Services

Kevin Jonkers
Director Cyber Risk Services

Bob Derix
Research specialist Markteffect

We would also like to thank the rest of the survey team, and the many others who contributed their ideas and insights into this report.

Contacts

Niels van de Vorle
Partner Cyber Risk Services
Email: nvandevorle@deloitte.nl
Tel: +31 (0)88 288 2186

Jurrien Mammen
Partner Cyber Risk Services
Email: jumammen@deloitte.nl
Tel: +31 (0)88 288 2507

Dana Spataru
Partner Cyber Risk Services
Email: dspataru@deloitte.nl
Tel: +31 (0)88 288 6623

Annika Sponselee
Partner Cyber Risk Services
Email: asponselee@deloitte.nl
Tel: +31 (0)88 288 2463

Martijn Knuiman
Partner Cyber Risk Services
Email: mknuiman@deloitte.nl
Tel: +31 (0)88 288 2941

Frank Groenewegen
Partner Cyber Risk Services
Email: fgroenewegen@deloitte.nl
Tel: +31 (0)88 288 1938

Hokkie Blogg
Partner Cyber Risk Services
Email: hblogg@deloitte.nl
Tel: +31 (0)88 288 5465

Guus van Es
Partner Cyber Risk Services
Email: guvanes@deloitte.nl
Tel: +31 (0)88 288 6677

Taede Rakhorst
Partner Cyber Risk Services
Email: trakhorst@delotte.nl
Tel: +31 (0)88 288 0718

Rob Stout
Partner Cyber Risk Services
Email: rstout@deloitte.nl
Tel: +31 (0)88 288 2398

Rob Wainwright
Partner Cyber Risk Services
Email: rwainwright@deloitte.nl
Tel: +31 (0)88 288 0032

Deloitte.

Designed by CoRe Creative Services. RITM0611847