Deloitte.

# Financial Cyber Survey

May 2021

# Editorial

The financial sector is generally known for having a high cybersecurity maturity level, due to having been at risk of cyber-attacks for several decades. However, financial businesses must be careful not to rest on their laurels, and they must continuously test assumptions about their cybersecurity posture and close any gaps between these assumptions and their aspirations as well as regulations.

In this survey, we investigate the Danish financial sector's ability to respond to cyber threats. The survey provides unique insights into the cybersecurity practices in the sector and reveals some major trends:

**The cyber threat has continued its increase.** And phishing remains the number one way to penetrate organisations, according to the respondents. The financial sector has been "in the game", so to speak, for several decades – cyber criminals have always sought a financial gain. Thus, being exposed to cyber threats has been a condition for financial businesses for a long time. The shape of the threat has changed, though. Today, it is not only about stealing money, but sometimes also about doing damage just for the sake of damage.

**Businesses might have a false sense of security.** The businesses in the sector have quite positive self-images when it comes to how close they are to being ideal cybersecurity organisations. Maybe a bit too positive as only one out of ten businesses have fully implemented what is generally considered baseline cybersecurity measures. While it is good to see that the businesses aspire to have high cyber maturity levels, we strongly recommend testing these assumptions and maturity levels independently and closing any gaps between the self-evaluations and the independent assessments.

**Many find it difficult to comply with cyber regulations.** No less than one third of the businesses in our survey indicate this. Indeed, compliance can be a complex task. Businesses within the financial sector need to adhere to a multitude of regulations and take into account multiple regulators that are not always aligned. But businesses should be ahead of regulations instead of chasing them. This not only gives them an advantage in terms of cybersecurity but is also far less costly.

In summary, the Danish financial sector continues to believe that it is higher up the cyber maturity ladder compared to other less mature industries. That may be the case. This should, however, not lead to complacency, which could result in these organisations falling behind the curve in the cyber-arms race.

We hope you will find this survey interesting. Please do not hesitate to contact us for further information.

**Hinko van Beek**
Partner
+45 30 93 52 57
hvanbeek@deloitte.dk

**Jay Choi**
Partner
+45 30 93 41 92
jaychoi@deloitte.dk

# The perceived cyber threat has increased – but the sector is used to the threat

The cyber threat has increased according to the respondents. However, many also report of an unchanged threat level which might be explained by the sector's relatively high level of cybersecurity maturity.

**What does the survey show?**

Three out of four respondents in the survey think that the cyber threat against their business has increased or increased significantly over the last two years. The remaining respondents report of an unchanged threat level. Nobody is of the perception that the cyber threat has decreased.

The businesses in the survey were asked about their perception of the development in the cyber threat level during COVID-19 (the survey was conducted in August 2020). Thirty-four percent indicate that the threat has increased during this period, and 66% indicate that the level has stayed the same. Again, nobody is of the perception that the threat has decreased.

**Deloitte's perspective**

Most of the respondents are of the perception that the cyber threat has increased over the last couple of years. However, compared to other sectors that have been investigated as part of Deloitte's Cyber Surveys (the consumer sector, the public sector and the energy, resources and industrials sector), the financial sector has a high proportion of respondents indicating that the threat level has remained unchanged over the last two years.

"I would not necessarily say that the threat has changed. We had the first couple of big attacks, and then media attention changed."

*CISO, global financial services provider*

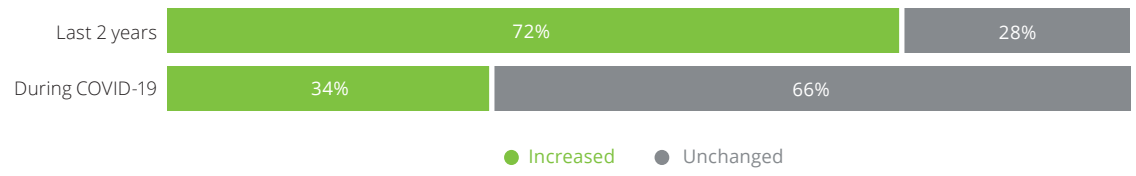
It is important to be aware of the distinction between the actual cyber threat level and the perceived cyber threat level. As this is a survey, the numbers reflect the perceived level. This could be part of the explanation why a relatively big proportion of the businesses in the financial sector sees the threat level as unchanged. Compared to the other sectors, the financial sector has a high cybersecurity maturity level in general, having been "in the game" and at risk of cyber-attacks for many years – people have always been after a financial gain. Thus, being exposed to cyber threats is a condition for businesses in the financial sector, and they have learned to live with it. They are more aware, and it does not feel like an increase.

However, the shape of the threat against the financial sector has developed over the years. Today, it is not only about obtaining a financial gain from financial businesses. Sometimes, the sole purpose of the attack is destruction.

"The financial sector has always been exposed to cyber-attacks, and it is not only about stealing our clients' money, but also about doing damage just to do damage."

*CRO, financial services provider*

*How has the cyber threat against your organisation in your view developed?*






**Financial Cyber Survey** | May 2021

# Cybersecurity is a natural part of the top management's agenda

Cybersecurity is frequently discussed by the top management. The increasingly tighter cyber regulations might have made the businesses in the sector prioritise the agenda.

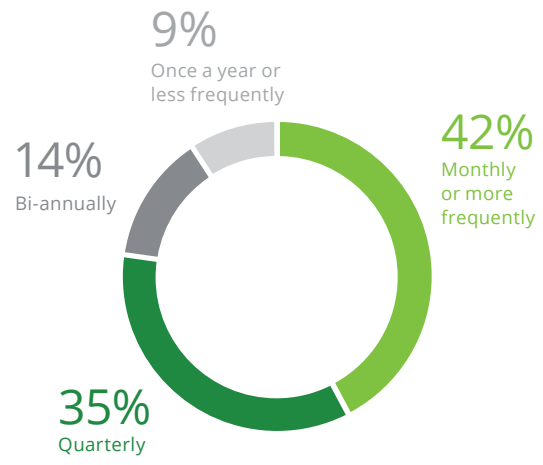
**What does the survey show?**
Forty-two percent of the respondents indicate that cybersecurity is on the leadership agenda monthly or more frequently. Thirty-five percent discuss cybersecurity in the boardroom on a quarterly basis, while 23% indicate that cybersecurity has the top management's attention twice a year or less frequently.

**Deloitte's perspective**
Cyber threats pose a significant risk to today's businesses. Therefore, it is positive to see that cybersecurity is a topic for the C-level executives and the boards in the businesses in the financial sector. Seventy-seven percent of the respondents in the survey indicate that cybersecurity is on the leadership agenda on a quarterly basis or more frequently.

The top management of the businesses in the financial sector is more focused on cybersecurity than the top management of the businesses in the other sectors that we have surveyed. This is no surprise, as cybersecurity has long been an eminent part of the financial sector's business operations, e.g. in the context of fraud detection and prevention. This combined with the increasingly tighter cyber regulations in the financial sector may have made the financial sector prioritise the cybersecurity agenda. The topic has become a natural part of the leadership agenda.

It is important to stress that frequency is not the only criterion for prioritisation; yet, it is likely that a higher frequency offers opportunities for making more informed decisions due to a generally improved understanding of the cybersecurity landscape, and for aligning investments accordingly.

*How often is cybersecurity on the top leadership's agenda?*




"Our board is asking a lot about cybersecurity and if we need more resources."

*CISO, global financial services provider*

# Phishing is considered the biggest risk

As many of the businesses in the financial sector are dealing directly with other people's money, phishing naturally has the attention of the sector.

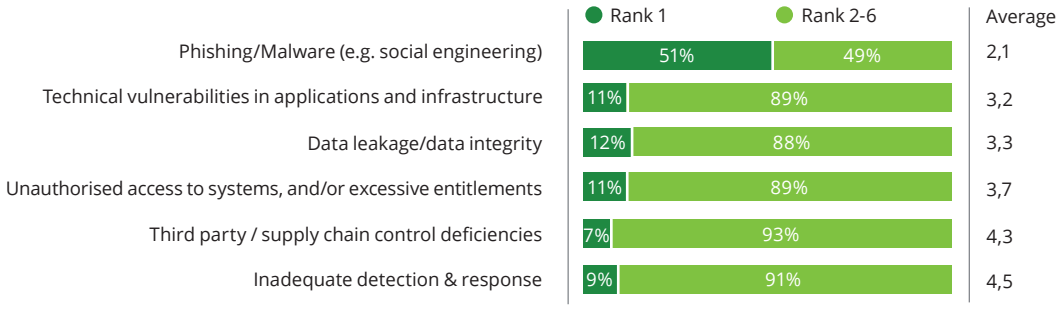
**What does the survey show?**
The survey shows that phishing/malware (e.g. social engineering) is considered the biggest cyber risk among the businesses in the financial sector. Half of the respondents have ranked this as the number one risk. The second biggest risk is, according to the average ratings, technical vulnerabilities in applications and infrastructure, and the third biggest risk is data leakage/data integrity.

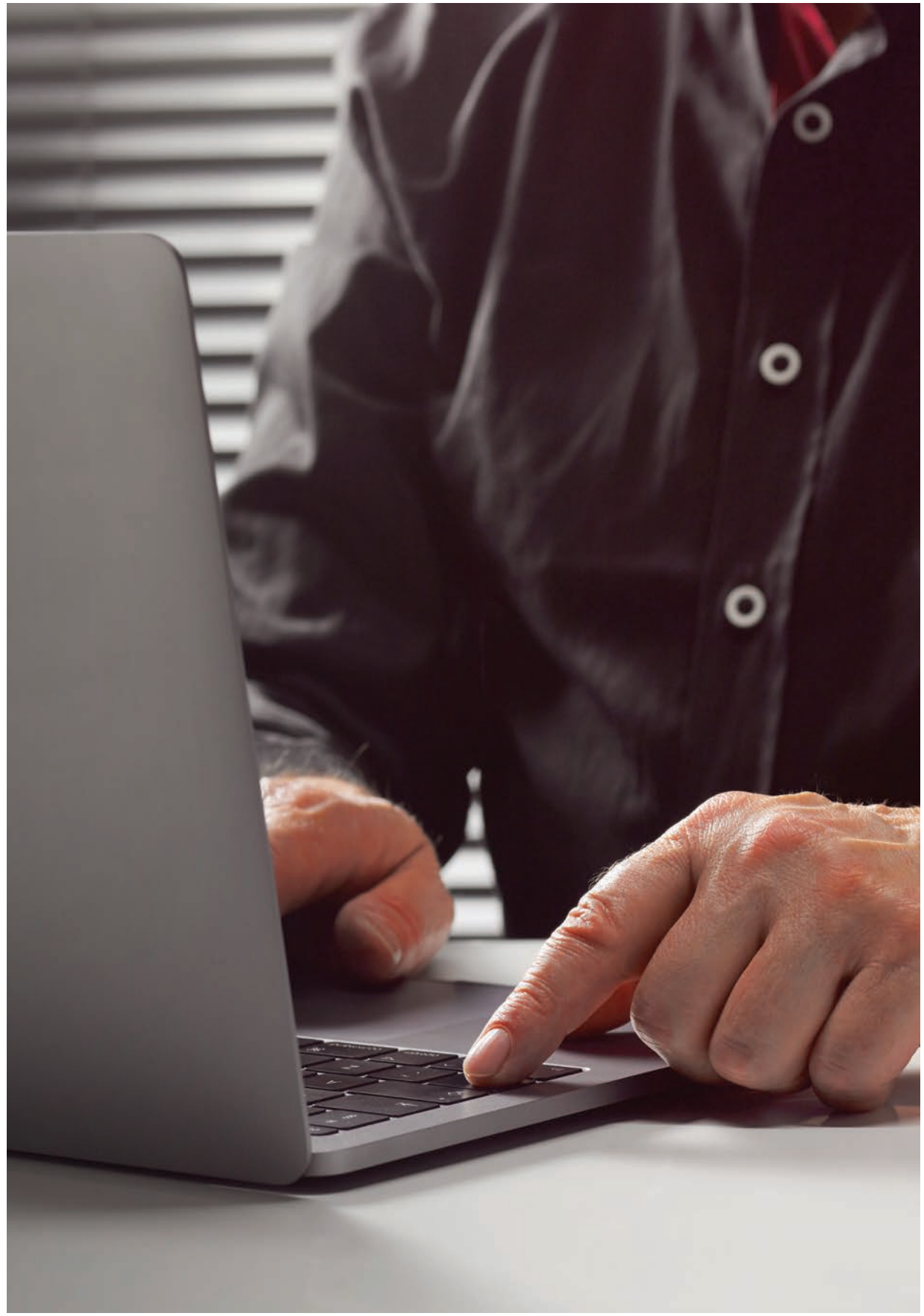
**Deloitte's perspective**
It does not come as a surprise that phishing is considered the number one cybersecurity risk by financial businesses. Phishing has been an effective channel for cyber-attackers; either as a means to introduce malware into an organisation's systems or directly leading to fraud via transfer of funds, e.g. using unsuspecting consumers' bank account details. The latter is somewhat specific to the financial sector and it has been a focus area especially for the banks for several decades now.

"In general, we are probably most exposed to phishing attempts, having somebody lurking around and pulling information from us."

*Head of Risk & Security, company in the financial sector*

*Rank these cybersecurity threats from 1-6, with 1 posing the greatest threat to your business and 6 being the smallest*



# Basic cyber defence efforts are lacking

Only one out of ten businesses have implemented all four baseline cybersecurity measures: response plans, self-defence plans, cyber awareness training and cyber hygiene.

**What does the survey show?**
Typical baseline cybersecurity measures include response plans, self-defence plans, cyber awareness training and cyber hygiene.

Fifty-three percent of the respondents indicate that they have a fully implemented self-defence plan, and 44% indicate that they have a fully implemented response plan. Forty-three percent of the respondents say that they conduct regular awareness training, and 37% say that cyber hygiene is fully implemented. Only 9% of the respondents indicate that they have all four cyber measures fully implemented.

**Deloitte's perspective**
As investments in new technology grow, so does the potential attack surface, enabling cyber criminals to exploit weaknesses. Therefore, it is alarming that only around one out of ten businesses in the financial sector have implemented all four baseline cybersecurity measures. In an increasingly digitised and interconnected world, it is crucial that businesses are protected by robust and resilient cybersecurity defences. The number is also surprising given the positive self-evaluation elsewhere in the survey where 72% have rated the level of their own cyber-security as 7 or higher on a scale from 0 to 10, 10 being the most mature. Thus, there is a risk of the businesses overestimating their own cybersecurity capabilities, operating with a false sense of confidence in their cyber defence.

"We are very afraid of breaching GDPR. Our company is based on systems that were designed way before GDPR."

*CRO, financial services provider*



**Financial Cyber Survey** | May 2021

"The most important defence mechanism of the banks are the employees – a human firewall."

*Head of Risk & Security, company in the financial sector*

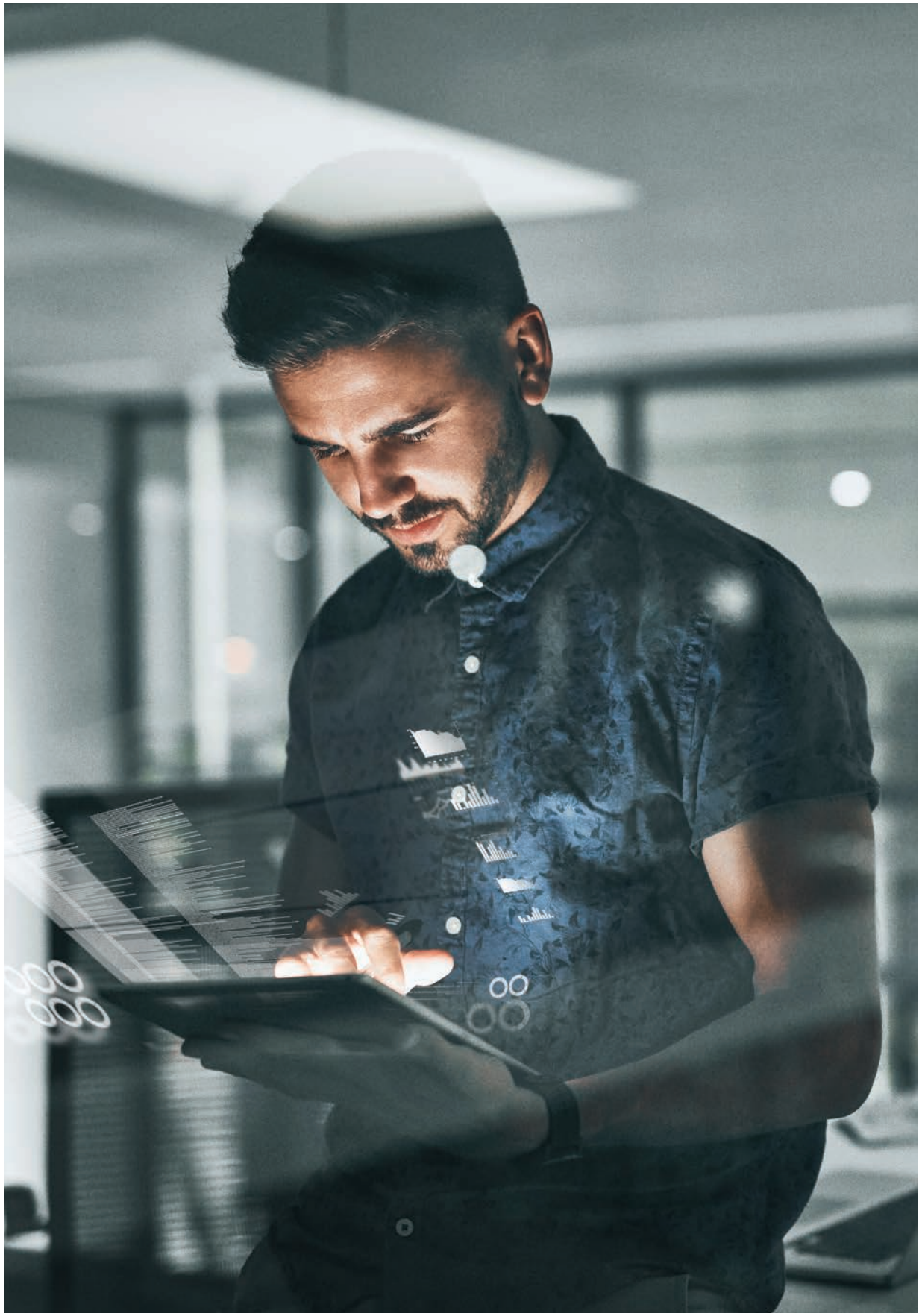
According to Deloitte's cyber experts, cyber hygiene and awareness training are fundamental and elementary initiatives that are crucial to any organisation's cyber resiliency. Also, it is a necessity to have both a strategic plan and an operational plan for how you should defend yourself against the threats you are facing. If you do not have a response plan that tells you how to act when a cyber-attack strikes you, you are not as resilient as you might feel you are. Ideally, such plans need to be in writing, and you need to test them frequently to make sure that you are ready for when – not if – your organisation is hit by a cyber-attack.


*Are all four cyber measures fully implemented in your organisation?*

There are plenty of low-hanging fruits that can be harvested relatively easily to strengthen cyber defence and resiliency. For instance, many organisations need to operationalise the knowledge, plans or procedures that already exist within the organisation but have not yet been documented or tested.

"We have a security incident response team which is a 24/7 function that monitors and reacts to security incidents."

*CISO, global financial services provider*



# Security-by-design: On the right track

Not incorporating security-by-design is costly and puts the business in a vulnerable position. The sector has come a long way, but still needs to be better at including cybersecurity from the get-go.

**What does the survey show?**
When asked about the development of their latest digital solutions, almost half of the respondents indicate that cybersecurity was taken into account before the actual development of the solution. Forty percent indicate that they started taken cybersecurity into account during the development or before implementation, while 10% say that this happened as part of or after implementation. None of the respondents say that cybersecurity was not taken into account at all. Two percent indicate that they had not taken cybersecurity into account until an actual cyber-attack (or attempt) prompted them to.

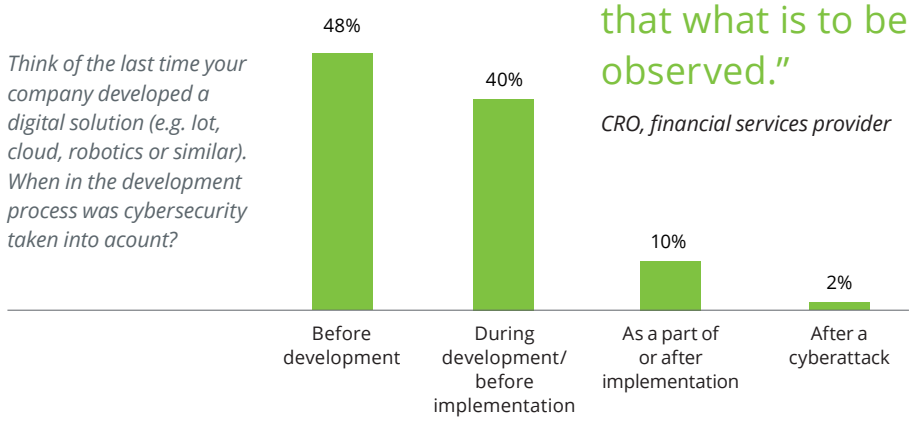
**Deloitte's perspective**
Businesses need to be proactive in their approach to cybersecurity. It is costly and ineffective not to take cybersecurity into account from the beginning in all design and system-development processes. Half of the respondents indicate that cybersecurity is taken into consideration before the actual development of the solution. This is positive and it supports the general trend that we have seen in the past 10 years, with cybersecurity having gone from not being considered at all to now being recognised as an instrumental part of product and system-development processes. We have come a long way when it comes to security-by-design, and it is important to recognise this positive development.

However, half of the respondents are not doing security-by-design – taking cybersecurity into account before actually starting the development of a solution. This number is too high. Not only does this increase the business' vulnerability; in many cases, it also makes the solution more expensive, especially if the security efforts need to be integrated once the solution has been implemented. Our qualitative data suggest that businesses really have the intention of getting better within the area. When asked about what would make them rank their own general cybersecurity higher, respondents pointed to exactly this – getting better at taking cybersecurity into consideration from the beginning.

"We have what we call a design authority board that aims at screening everything to ensure that what is to be observed is observed."

*CRO, financial services provider*

*Think of the last time your company developed a digital solution (e.g. Iot, cloud, robotics or similar). When in the development process was cybersecurity taken into acount?*



# Businesses, be ahead of regulations!

There is a multitude of regulations that the businesses must comply with. But being ahead of regulations instead of chasing them gives the businesses an advantage and is far less costly.

**What does the survey show?**

Forty-seven percent of the respondents indicate that they are highly able to comply with the government's cyber regulations within IT privacy and cybersecurity (e.g. GDPR, cyber data privacy and outsourcing). Forty-one percent indicate that they are able to do this to some degree, and 1% to a lesser degree. No one is of the perception that they are not able to comply at all, and 10% indicate that they don't know.

The respondents were also asked if they find it easy or difficult to comply with these regulations. Twenty-nine percent find it easy, 32% find it difficult, and 37% find it neither difficult nor easy. No one finds it very difficult, and only 1% find it very easy.

**Deloitte's perspective**

The proportion of businesses indicating that it is difficult to comply with government regulations is high – one third (no one finds it very difficult, though). Part of the explanation could be that regulations can be complex. There is a multitude of regulations that businesses within the financial sector need to adhere to and multiple regulators - that are not always aligned - to take into account.

The respondents were also asked about the effects of these regulations. There is a group of respondents that indicate that the regulations have resulted in an increased focus on cybersecurity in their organisation. Some of them indicate that the regulations have provided them with a framework for working with cybersecurity. Other respondents point to the stick effect of the regulations – getting fined if regulations are not complied with.

Then, there is a group of respondents indicating that the regulations have increased the bureaucracy.

"We are regulated in a large number of countries, directly or indirectly. That of course gives a lot of complexity in terms of the compliance piece."

*CISO, global financial services provider*





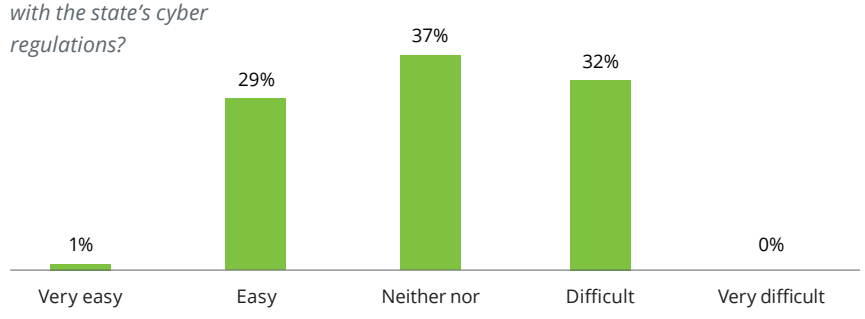
Some point to more administrative work. Others say that the regulations have made things more difficult, as they do not always agree with the regulations.

Not all of the businesses surveyed, however, see the regulations as having an impact. They indicate that they would have taken the measures anyway. This is positive. Businesses should be ahead of regulations instead of chasing them and being worried about them. This not only gives them an advantage in terms of cybersecurity but is also far less costly.

"I think we are doing well on complying with cyber regulations. That is our ambition, at least."

*CISO, global financial services provider*

*How easy or difficult do you find it to comply with the state's cyber regulations?*



# A positive self-image – but it is too positive?

The businesses rank themselves high when asked about their closeness to the ideal cybersecurity organisation. The sector is indeed very mature within the area, but do they paint too positive a picture?

**What does the survey show?**
In the survey, we asked the respondents to envision an ideal organisation where cybersecurity is deeply rooted; cyber and information security resources are adequate; and thorough threat assessments and contingency plans are in place. The respondents were then asked to indicate how close their organisation is to this ideal on a scale from 0 to 10 (10 being the ideal organisation).

The average self-evaluation is just about 7. Seventy-two percent of the respondents rate themselves 7 or higher. Seven percent rate themselves as 5 or below.

"We are a seven. Other organisations have a more mature setup. We have some work ahead of us."

*Head of Risk & Security, company in the financial sector*

"We know we have gaps. But that is also part of our maturity, right? Knowing where our gaps are, and what it takes to reduce them."

*CISO, global financial services provider*

**Deloitte's perspective**
The businesses in the financial sector have a quite positive self-image when it comes to how close they are to being an ideal cybersecurity organisation. While the average for the businesses in the financial sector is just around 7, the average for all four sectors in Deloitte's Cyber Surveys (consumer sector, public sector and energy, resources and industrials sector) is around 6.

The financial sector is a bit more mature than the other sectors when it comes to cybersecurity. However, generally speaking – and in our experience – self-evaluations tend to paint too positive a picture. This could also be the case with the surveyed businesses. While it is good to see that the businesses aspire to be at the high cyber maturity levels, we strongly recommend testing these assumptions and maturity levels independently and closing any gaps between the self-evaluations and the independent assessments.



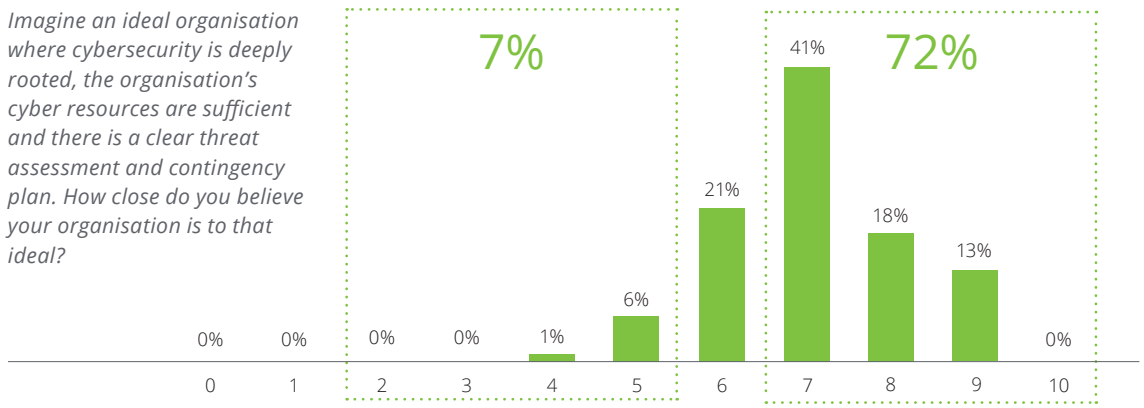


"We are a five. It is all about integrating it by design - security, privacy and so on."

*CRO, financial services provider*

To some extent, the positive self-evaluation also stands in contrast to the fact that less than one out of ten businesses in the financial sector have fully implemented baseline cybersecurity measures (response plans, self-defence plans, cyber awareness training and cyber hygiene) – as asked about elsewhere in the survey.

*Imagine an ideal organisation where cybersecurity is deeply rooted, the organisation's cyber resources are sufficient and there is a clear threat assessment and contingency plan. How close do you believe your organisation is to that ideal?*



# A value chain is only as cyber resilient as its weakest link

Cyber-attacks have become a question of when they will occur - not if. Having a resilient cyber defence in place is essential as it enables businesses to rapidly respond to and recover from cyber-attacks suffering minimal damage.

**What does the survey show?**
The respondents indicate that they are quite cyber resilient within the areas of handling customer data and marketing/sales. Ninety percent of the respondents indicate that they are highly or to some degree cyber resilient within these two areas. For the other key areas shown in the graph on the next page, the percentage of businesses indicating that they are highly or to some degree resilient is between 83% and 88%.

"To be honest, what I am fearing the most is not what I am in control of, but what I am not in control of. And that is not our third-party vendors. It is our clients."

*CISO, global financial services provider*

There are differences, however. While 53% indicate that they are even highly resilient when it comes to handling customer data, the percentage is only 29% when it comes to new technology. Eight percent indicate that they are not cyber resilient at all when it comes to the use of close business partners/suppliers (with system integration).

**Deloitte's perspective**
Compared to other sectors, the businesses in the financial sector rate their own cyber resiliency lower in general. Once again, part of the explanation could be that the businesses in the financial sector are more aware of the cyber threat because of their maturity. They have been exposed to cyber threats for a long time due to the nature of the business and are thus more realistic about it all, including their own resiliency.

The FinTech (financial technology) companies aside, the financial sector has not been as adaptable and accommodating as regards digital transformation due to internal and external challenges. This might have

”When it comes to handling customer data, our resiliency could be better. We have had an unfortunate incident. However, in relation to GDPR, I would not say the biggest risk is cyber, it is our own actions.”

*CRO, financial services provider*

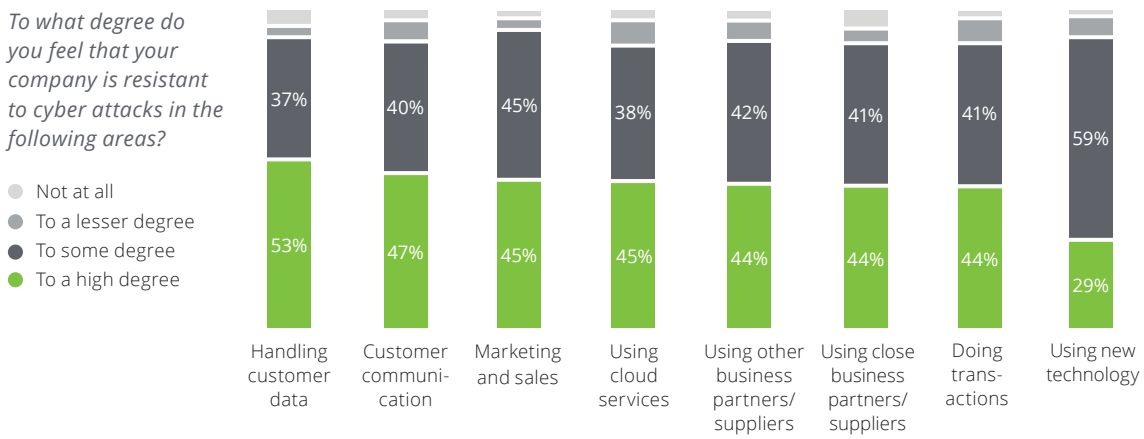
made the financial sector feel less cyber resilient in terms of new technology.

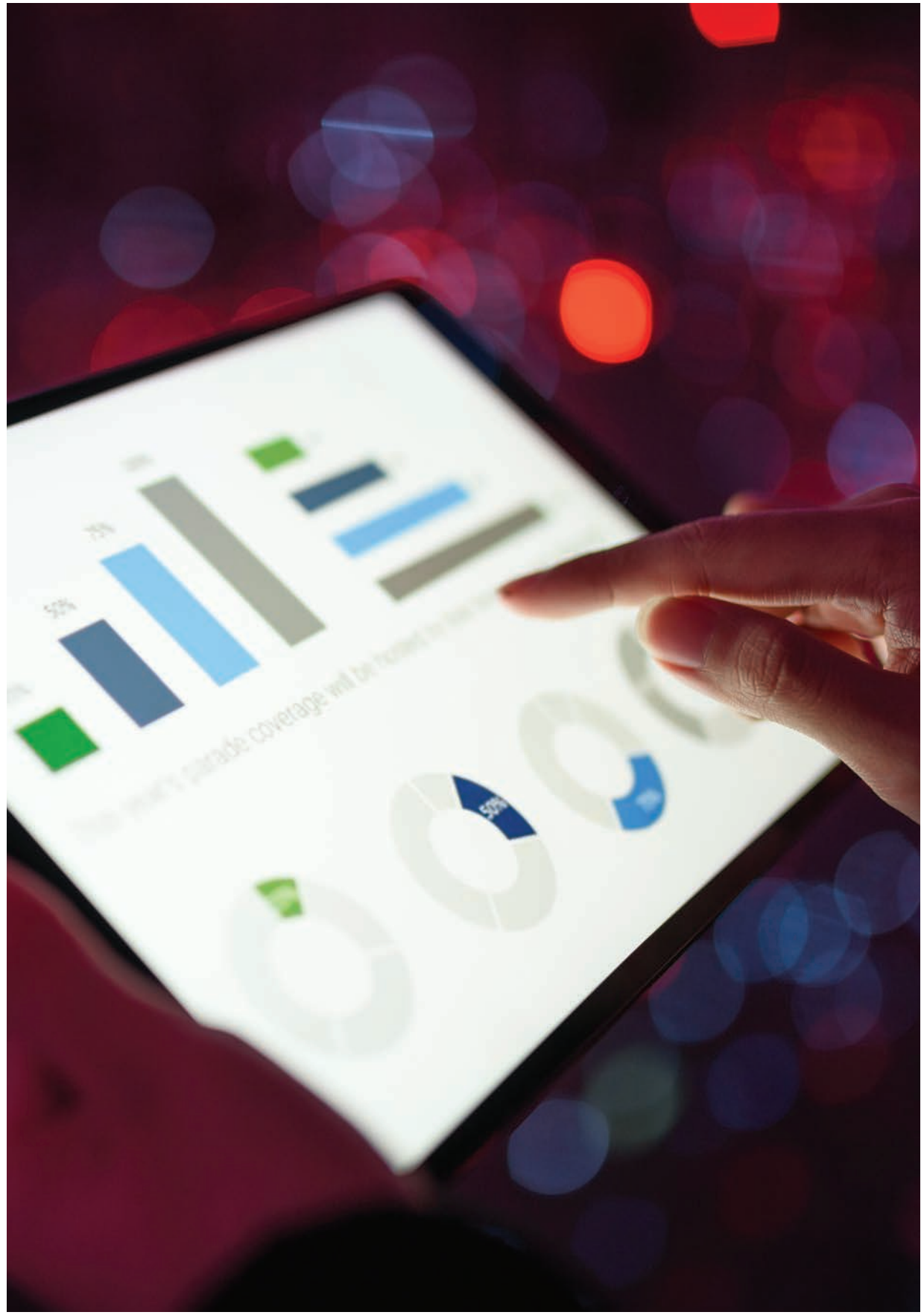
The survey shows a high level of perceived cyber resiliency when it comes to handling customer data. This is a positive development that can possibly be accredited to EU’s General Data Protection Regulation (GDPR) combined with an increased focus on data privacy and general compliance with privacy regulations. It is promising to see that the increased focus on and awareness of privacy issues have also led to increased confidence in handling and protecting customer data. Seven percent of the businesses in the financial sector, however, indicate that they are not resilient at all when it comes to handling customer data.

“We are very resilient. That is the ambition, at least.”

*Head of Risk & Security, company in the financial sector*

*To what degree do you feel that your company is resistant to cyber attacks in the following areas?*



# Being proactive and attractive helps recruitment

The competition is fierce when it comes to the recruitment of cyber capabilities. A proactive approach and being able to offer people to work in a tech-driven environment serve as key advantages for the sector.

**What does the survey show?**
When it comes to attracting new employees with competencies within cyber and information security, 21% of the respondents indicate that they find this easy (nobody finds it very easy, though). Twenty-two percent find it difficult or very difficult, and 57% indicate neither nor.

Twenty-two percent of the respondents indicate that they find it easy or very easy to retain these employees. Lastly, when it comes to developing current employees' competencies within cyber and information security on a regular basis, 31% answer that they find this easy or very easy.

**Deloitte's perspective**
The financial sector has a relatively good ability to attract employees with cybersecurity capabilities. An explanation for this could be that businesses in this sector often are able to pay a relatively high salary. A complimentary explanation could be that the businesses in the sector are very aware that the competition for cybersecurity capabilities is fierce. Combined with a desire to be "best in class", the businesses take on a very proactive approach and are putting a lot of effort into attracting employees.

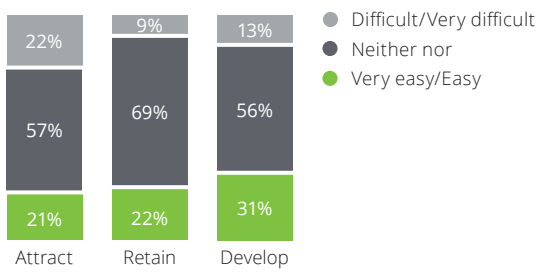
The picture is mixed, however. About one out of five businesses in the survey find it easy to attract employees with cybersecurity capabilities. But an equal proportion finds it difficult or even very difficult. This split in opinion might have something to do with the type of capabilities: You can find the generalists relatively easy, but it is harder to find the specialists with the deep understanding and competences (e.g. incident response professionals, security architects, and C-level strategy consultants). A point from the qualitative data is that the pool of talent in Denmark is too small, not least when it comes to the specialists. Therefore, it is often necessary to look abroad for these skills.

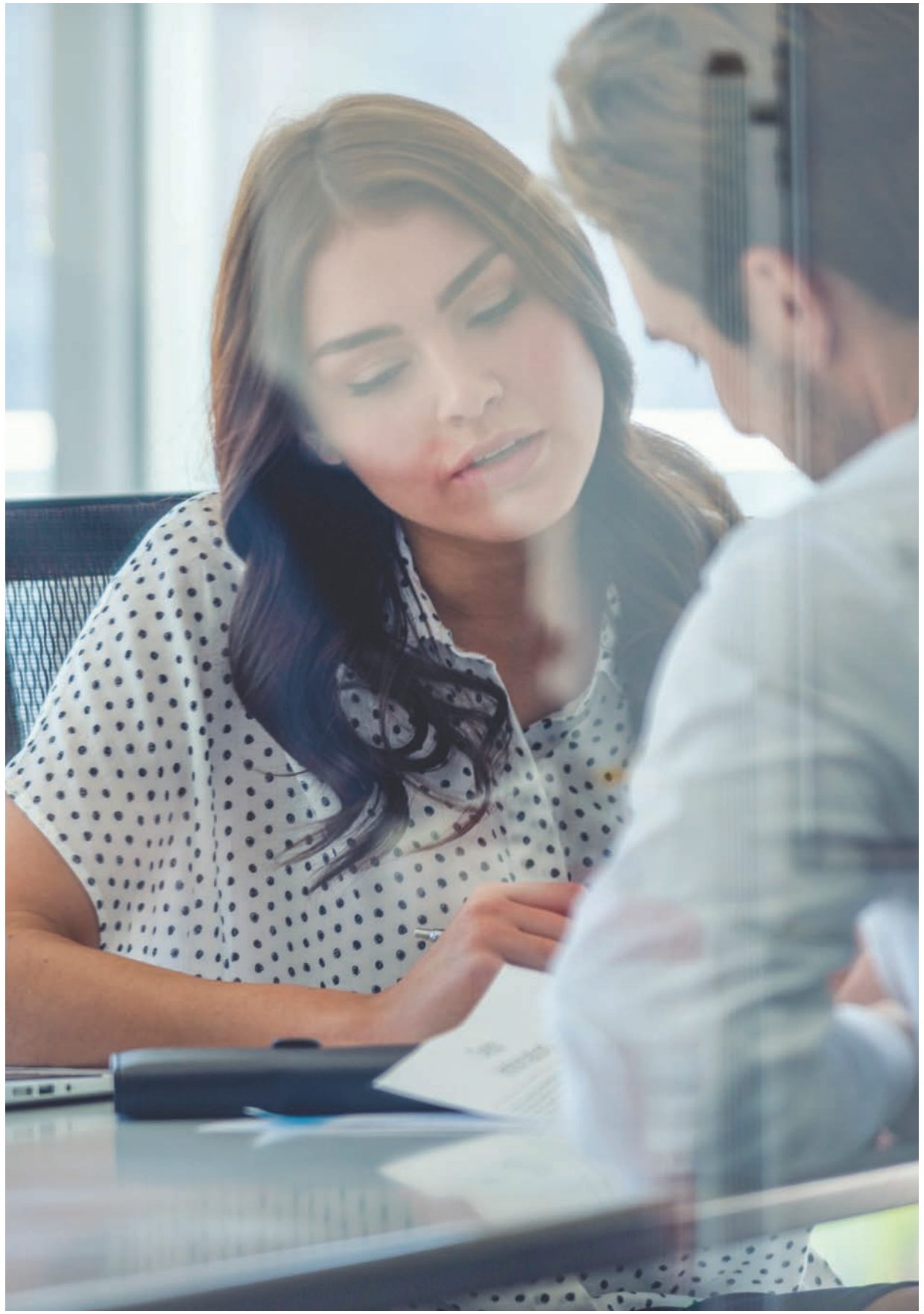
Different sectors have different advantages when it comes to attracting and retaining employees with cyber capabilities. Where sectors such as the public sector and the energy, resources and industrials sector might be able to take advantage of people wanting to serve a higher purpose, our qualitative data suggest that the financial sector might be able to take advantage of offering people to work in a more tech-driven environment – giving people the opportunity to work innovatively and with technical challenges.

"Attracting the right talents is hard because the pool of people is small."

*CISO, global financial services provider*

*How easy or difficult do you find it to attract/retain/develop employees with competencies within cyber and information security to/within your organisation?*



Deloitte.

Deloitte leverer ydelser indenfor revision, consulting, financial advisory, risikostyring, skat og dertil knyttede ydelser til både offentlige og private kunder i en lang række brancher. Deloitte betjener fire ud af fem virksomheder på listen over verdens største selskaber, Fortune Global 500®, gennem et globalt forbundet netværk af medlemsfirmaer i over 150 lande, der leverer kompetencer og viden i verdensklasse og service af høj kvalitet til at håndtere kundernes mest komplekse forretningsmæssige udfordringer. Vil du vide mere om, hvordan Deloittes omkring 312.000 medarbejdere gør en forskel, der betyder noget, så besøg os på Facebook, LinkedIn eller Twitter.