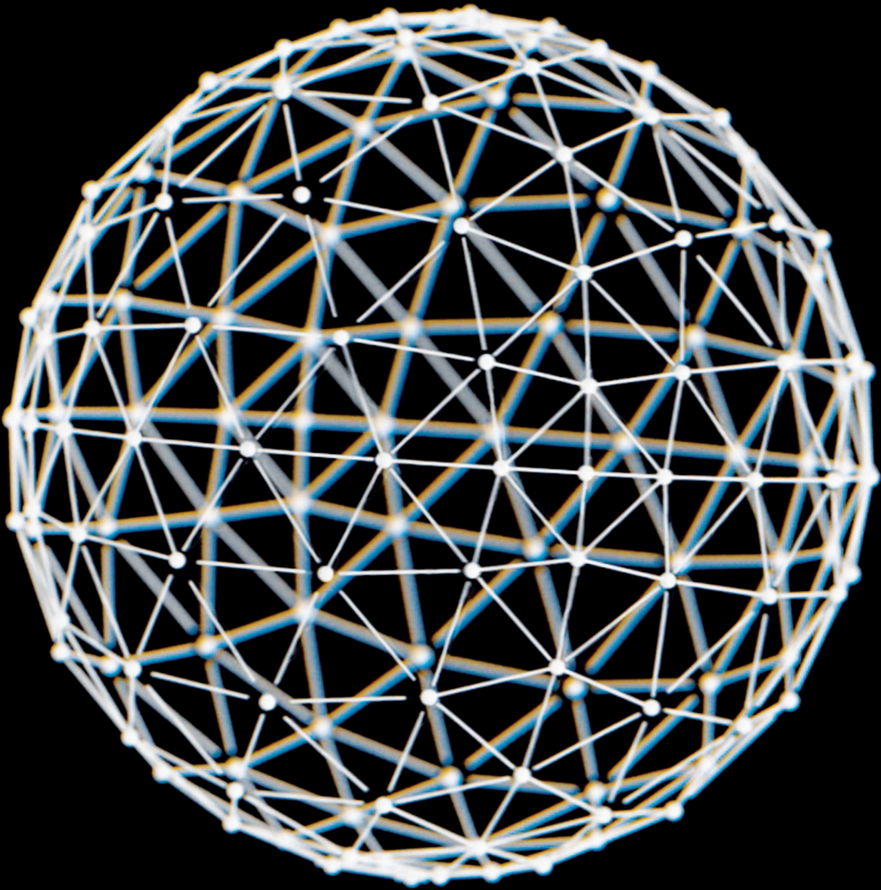
Deloitte.



Consumer Cyber Survey

September 2020

Editorial

During the last few years, consumer businesses have been in for a rude awakening in terms of cybersecurity. From strict regulations, such as the European General Data Protection Regulation (GDPR) to crippling cyber-attacks, including the infamous NotPetya, it has been necessary for businesses to change their understanding of what it takes to stay ahead of the curve in cyber. It is yet to be seen whether these events have brought any meaningful change to the industry. This survey aims to provide a sneak peek.

In this survey, we focus on the consumer businesses in Denmark and especially the sector's ability to respond to the ever-increasing cybersecurity regulation and threats. Our study uncovers three major trends that may shed some light:

There is increased awareness of cybersecurity. It is no surprise that consumer businesses are more alert to cyber-attacks with several high-profile incidents reported in recent times. This has led to increased senior management attention to cybersecurity; yet, this seems to be a temporary interest linked to news coverage rather than a lasting, true understanding of the underlying problem.

There is also increased confidence, which may be misleading. With increased awareness, we have also seen an increase in self-confidence in terms of consumer companies' perception of their cyber capabilities, e.g. how close they are to an ideal setup. This is surprising, given that several attacks have only recently exposed the same companies' lack of preparedness and low maturity regarding the subject. We urge companies to be mindful of this false sense of security.

There are still several low-hanging fruits available for improvement. Similar to our survey on the public sector, there are several fundamental solutions that Danish consumer companies can implement to improve their cyber resiliency. These are "no regrets" capabilities that we expect every company to implement to a certain degree to firmly establish their security baseline.

In summary, it seems that Danish consumer companies have learned from regulations and cyber-attacks in the past few years but are yet to implement meaningful change for a lasting effect. What is alarming is the increasing self-confidence, which may be the result of increased awareness rather than actual cyber capability.

We hope you find this survey interesting. Please do not hesitate to contact us if you would like further information.

Henrik Andersen
Partner
Tlf: 20 48 12 29
andersenh@deloitte.dk

The perceived cyber threat has surged during the last two years

According to insights from Deloitte's Cyber Intelligence Centre, COVID-19 has resulted in an increase in phishing and ransomware attacks. This development builds on the general acceleration of cyber threats we have seen during the last couple of years and is best exemplified by the impactful cyber-attacks suffered by major Danish consumer businesses.

What does the survey show?
72% of the respondents believe that the cyber threat against their organisation has either increased or increased significantly during the last two years. Looking back on the first months of the COVID-19 crisis, 43% of the respondents indicate that corresponding developments in the threat level have occurred. Even though there is a significant difference between these two figures, both figures represent a positive change in Danish consumer businesses' threat awareness level.

However, there is still room for improvement, which is exemplified by the 24% of the respondents stating that the cyber threat level has remained unchanged during the last two years, and the 54% indicating the same developments during the first months of COVID-19.

The survey also shows that, during the past year, one out of ten respondents has been exposed to a cyber-attack that has affected the economy, operations or/and reputation of their organisation. Further, another 16% have managed to detect such an attack and stop it in time. 70% have not been affected by a cyber-attack of this scale.

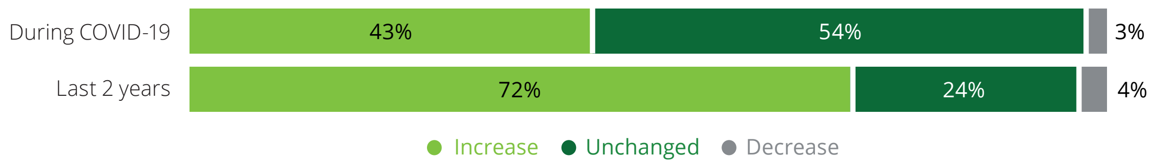
> "I believe we've improved, but we're far from where we should be. We're not moving fast enough compared to the threat level development".
>
> *CISO of a large, Danish consumer business.*

Deloitte's perspective
According to Deloitte's cyber experts, building a resilient cyber defence begins with a detailed threat assessment, weighing the likelihood of different threats and embedding prioritised security measures as a result. Altogether, this should form the basis of the strategy and budgeting and help you identify the competences necessary to keep the organisation safe.

The fact that 24% of the respondents do not perceive the threat level to have changed during the last two years, and that 54% have not experienced an increase during COVID-19 either, might indicate that it is necessary to revisit the cyber threat assessment for some Danish consumer businesses.

Having visibility into one's own organisation as well as having the needed resources available and access to sufficient data is crucial to having a realistic understanding of how the threat landscape looks like and evolves. By not having a realistic understanding of such developments, it becomes almost impossible to mitigate the threats one's organisation are facing. A mismatch between threats and cyber defence efforts poses a potent security risk.

Finally, 11% of the respondents indicate that they have been hit by a cyber-attack, which has affected their economy, operations and/or reputation during the past year. This is a high number, taking into account that another 16% have detected and stopped an attack of a similar scale, and that a noteworthy number of undetected incidents can be expected. This underlines how significant the cyber threat against Danish consumer businesses has become.



11%
Have been exposed to a cyber-attack (affecting economy, operations and/or reputation) during the last year.

16%
Have detected and stopped a potential cyber-attack (affecting economy, operations and/or reputation) during the last year.

70%
Have not been affected by a cyber-attack (affecting economy, operations and/or reputation) during the last year.

Attention please - cybersecurity has entered the leadership agenda

An increase in the overall cyber threat level combined with several critical cyber-attacks on major, international consumer businesses has elevated cybersecurity to the leadership and boardroom agenda.

Our survey shows that cybersecurity is frequently being discussed by top management in the Danish consumer businesses participating in the survey. However, the survey also reveals that there is still room for improvement in many organisations.

What does the survey show?

According to 37% of the Danish consumer businesses surveyed, cybersecurity is on the leadership agenda weekly or monthly. 28% discuss cybersecurity in the boardroom on a quarterly basis, while 35% indicate that cybersecurity has the leadership's attention twice a year or less frequently.

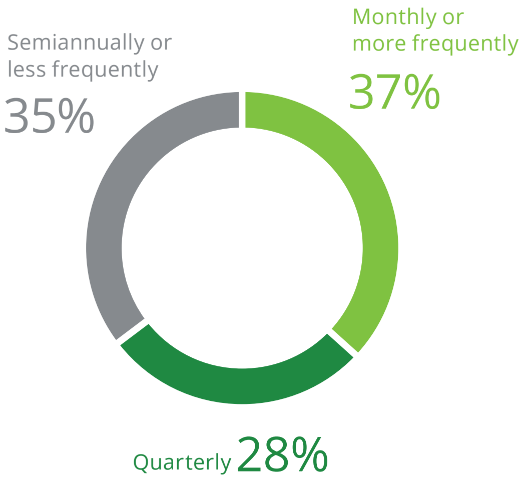
Deloitte's perspective

Cybersecurity poses a significant risk to today's businesses. Therefore, it is positive to see that cybersecurity is being prioritised and discussed by the leadership of Danish consumer businesses. What catalyses this increased prioritisation could be a growing cyber concern besides the obvious and well-known negative commercial impact of a cyber-attack. The growing concern might be a result of the high-profile incidents Danish and international consumer businesses have experienced during the last couple of years.

The question, however, is whether the prioritisation and boardroom discussions equal increased execution of necessary and critical cyber efforts. In Deloitte's experience, this shift from discussion to action still needs to mature. This is further supported by the below quote.

> "On an average basis, I'd say cybersecurity is on the agenda two times a year. That is not enough if you want to create a strong cyber culture in the organisation".
>
> *Information Security & Data Privacy Director of a large, Danish consumer business.*

The fact that 35% of the respondents indicate that cybersecurity is not on the leadership's agenda more than once or twice a year poses a significant threat to those businesses. Without having frequent discussions with IT managers and CISOs, it can be difficult for the top management to make informed decisions about efforts such as the cyber budget, risk appetite and the overall security level. It is critical that the leadership is informed regularly, but also that it is directly involved in the strategic cyber initiatives. The sudden surge in cyber-attacks during COVID-19 is a good example of why it is necessary to meet and discuss the cyber threat assessment regularly.



"I have never worked in a company that prioritise IT-security as high as we do. I meet with t he top management to discuss IT-security every week, and I perceive that as a big advantage".

CISO of a large, Danish consumer business.

"Well, I guess it's the same as in every other company - it's a topic we've a hard time getting on the agenda. But, because of the current circumstances, it is on the leadership's agenda right now".

Information Security Manager of a large, Danish consumer business.

Cybersecurity is on the leadership agenda on a monthly or more frequent basis in 37% of the surveyed businesses, on a quarterly basis in 28% of the surveyed businesses and on a semiannual or less frequent basis in 35% of the surveyed businesses.

Cybersecurity needs to be included from the get-go

The approach to cybersecurity has for a long time been more reactive than proactive – a costly and ineffective way to defend your business.

To match the ever-expanding threat landscape, businesses should be more proactive in their approach to cybersecurity. Cybersecurity should be considered from the start in all design and system development processes, and our survey indicates that the majority of the surveyed consumer businesses have realised this.

What does the survey show?
According to our survey, 67% of the respondents considered cybersecurity as one of the first things in the development process when developing their last digital solution. Almost 30% took cybersecurity into account during the development process or before implementing the digital solution, while 3% did so as part of or upon implementation. In 3% of the surveyed consumer businesses, cybersecurity was not being considered at all.

Deloitte's perspective
Cyber-attacks have become a question of when - not if - they happen, and this underlines the importance of having cybersecurity-by-design measures embedded as a standard element of every product, system and technology development process. By having cybersecurity incorporated as an integral part of the digital system or solution from the start, businesses increase their resilience and enhance their business continuity.

It is a positive change that close to 7 out of 10 of the respondents indicate that they considered cybersecurity prior to development the last time they developed a digital solution. This supports the general trend we have seen during 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. In recent years, this trend has been driven by EU's GDPR rules, further compliance requirements and a privacy-by-design focus, especially in terms of consumer businesses.

That said, it is difficult to decipher whether the results mean that proper cybersecurity efforts have actually been implemented, or if it was merely a single security review with no considerable effects. Data from our qualitative interviews supports the above-mentioned trend that cybersecurity has become an incremental part of the product and system development processes. The question, however, is whether these processes are embedded throughout the organisation, i.e. would product and project owners have the same understanding, or is it a result of our respondents' (cyber security responsibles) perspective?

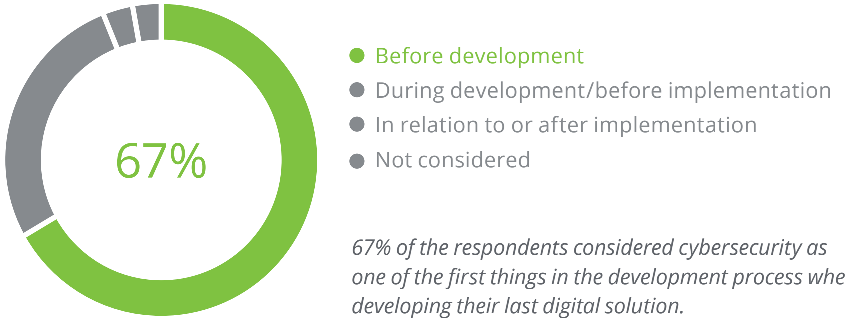
As we help Danish consumer businesses increase their cyber resiliency, we still see a significant number of products, services and systems that lack basic cybersecurity measures, with cybersecurity not having been considered in the initial development process. Not only does this increase the organisation's 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.

"Cybersecurity is included from the start. It already starts on the business side when we sign an agreement".

Security Manager of a large, Danish consumer business.

"Before we implement a digital solution, we've an IT security routine, but after that it all stops. We're doing this on an ad hoc basis, you could say".

Information Security & Data Privacy Director of a large, Danish consumer business



67% of the respondents considered cybersecurity as one of the first things in the development process when developing their last digital solution.

A supply chain is only as cyber resilient as its weakest link

Our world has become interconnected, and so have businesses and suppliers across the globe.

When you increase the number of parties in your supply chain, you are also increasing the potential attack surface of your business. Even though your cyber defence is sophisticated, your suppliers might not adhere to the same standards. The surveyed consumer businesses predominantly feel confident about their supply chains' cyber resiliency. However, there are also red flags.

What does the survey show?
According to the survey, 78% believe that their company is resilient against cyber-attacks to a high degree when it comes to handling customer data. 63% indicate the same level of cyber resiliency when it comes to using cloud services. Assessing their cyber resiliency in relation to suppliers, new technology and customer services, more than half of the respondents believe that they are cyber resilient only to some degree or to a lesser degree.

Deloitte's perspective
One of the things that stand out here is the alleged cyber resiliency when it comes to handling and protecting customer data. As previously mentioned, EU's GDPR combined with an increased focus on compliance with privacy regulations has been a decisive factor in driving this development, especially for consumer businesses.

It is promising to see that the increased focus and awareness have also led to increased confidence in handling and protecting customer data.

Another yet more alarming conclusion is that more than half of the respondents feel they are only to some degree, a lesser degree or not at all resilient in areas of the supply chain that involve business partners, suppliers and new technology. This causes concern, as we are currently experiencing an increase in attacks targeting the supply chain.

When cyber-attackers are targeting the supply chain, the large corporations remain the end-goal. By using the smaller suppliers as entry points and exploiting the weaknesses in their defence, however, it becomes easier for attackers to gain access to those large companies. The data from the survey is supported by the findings of the qualitative interviews, underlining the fact that suppliers and new technology seem to be a weakness in terms of the respondents' cyber resiliency.

As mentioned in the section about the surging cyber threat, 70% of the respondents state that they have not suffered a major cyber-attack during the last year.

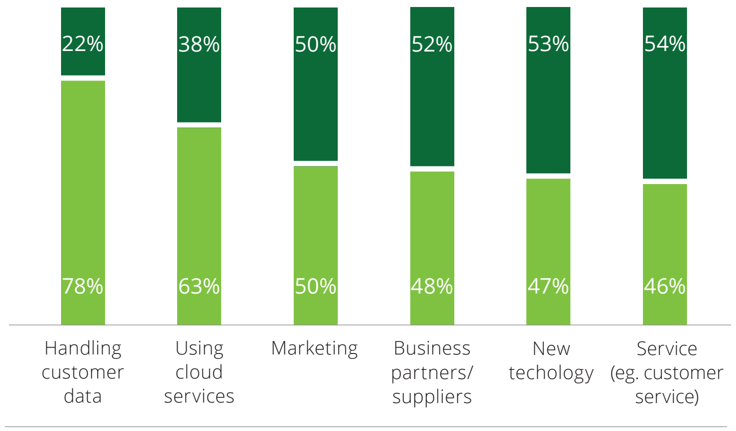
"We need to be more focused on increasing our resiliency when it comes to new technology. I don't think we're where we should be in this area".

CISO of a large, Danish consumer business.

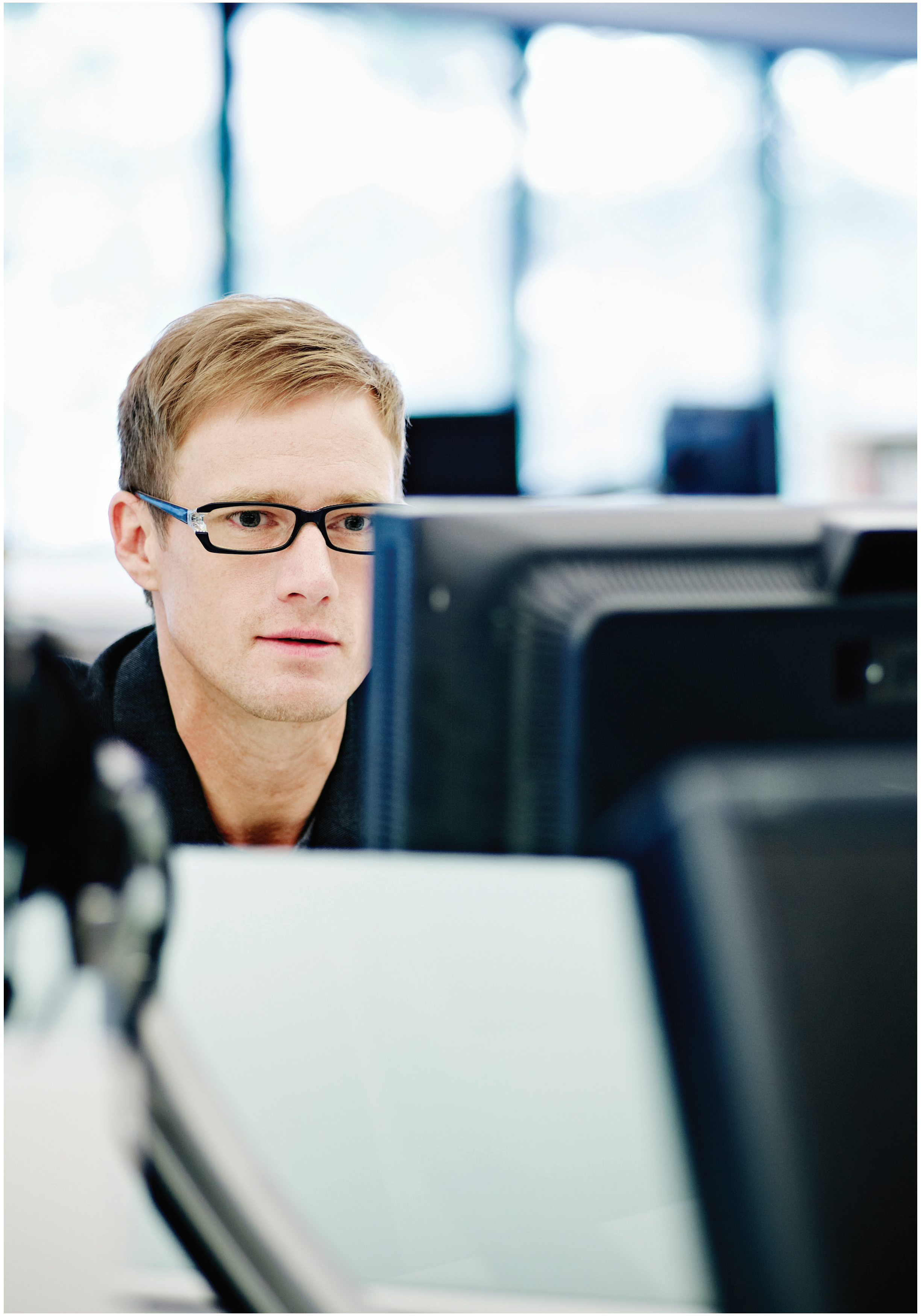
Yet, almost half of the respondents believe that they are resilient against cyber threats throughout the supply chain to a high degree. It is unclear what this assessment is based on, but it could indicate that some of the surveyed consumer businesses are operating under a false sense of confidence when it comes to their own cyber defence.

"As for suppliers, I have to admit that this is an area where we aren't very resilient yet. It's part of this year's roadmap and we need to start working on it".

CISO of a large, Danish consumer business.



78% believe that their company is highly resilient to cyber-attacks related to handling customer data. 63% indicate the same level of resiliency when it comes to using cloud services. Less than half feel resilient in areas that include suppliers, new technology and customer service.



Approaching the cyber ideal, but everything is not as good as it seems

In an ideal world, cybersecurity should be deeply rooted in every organisation and permeate every action and decision from the top management to the staff on the floor.

There should be a thorough understanding of what the threat landscape looks like and how it evolves; how to address the threats; and how to react when an incident occurs. According to the surveyed consumer businesses, the vast majority believe that they are close to this ideal.

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

Almost 3 out of 4 of the respondents believe that their organisation ranks 7 or higher, while only 16% rank their organisation 5 or below.

Deloitte's perspective
As we help Danish consumer businesses assess and evaluate their cybersecurity maturity, we often encounter organisations which lack a well-informed understanding of the current cyber threat landscape and which generally lack both defence and response plans as well as sporadic or non-existing awareness training. This cannot be characterised as being close to the ideal cyber organisation as depicted in the aforementioned description.

Considering some of the conclusions made from the survey so far, something could indicate that a significant number of the respondents have a somewhat false sense of confidence in their own cyber defence.

> "I would place us around 5, but if you take a deep dive into that assessment you will find that we rank 10 in some areas and 0 in others".
>
> *Information Security Manager of a large, Danish consumer business.*

> “We’re a 4 – we have a long way to go. I do, however, believe that we, in some areas, are doing okay compared to our peers”.

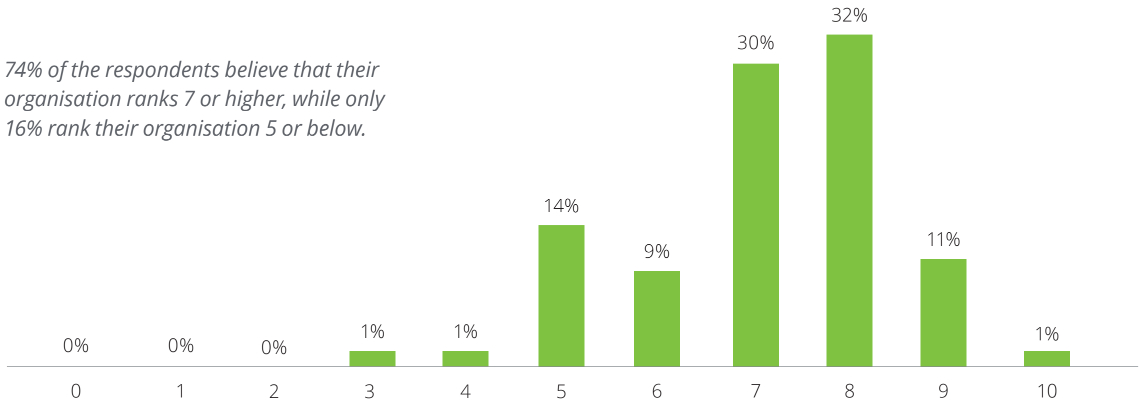
CISO of a large, Danish consumer business.

This argument is supported by the findings of our report, as almost 1 out of 4 perceive the threat level to have remained unchanged during the last two years. This is further supported by the finding indicating that more than half of the respondents feel that they are only partly, or not at all, resilient in their supply chain when it comes to suppliers and new technology. Finally, this is also supported by the fact that 35% of the respondents only discuss cyber with the top leadership twice a year or less frequently.

The highlighted quote is a good example of a common pitfall that can lull businesses into a false sense of security and make them counterproductive in terms of establishing a secure cyber environment. Benchmarking your peers against your own defence does not necessarily tell you enough about your own defence efforts – especially not if the industry tendency is that cybersecurity is not a priority. Indicating that you are below 5 out of 10, but doing okay compared to your peers, will assumingly tell you more about the lack of defence among your peers than about the state of your own defence.

Generally, self-evaluations tend to paint too positive a picture compared to what reality looks like. This could also be the case with the surveyed consumer businesses considering the respondents’ rather positive self-evaluations. Our experience shows that respondents from IT often have a more positive view on the security situation than respondents from distinct cyber teams.

74% of the respondents believe that their organisation ranks 7 or higher, while only 16% rank their organisation 5 or below.



Basic cyber defence efforts are lacking

With rising consumer demands and expectations, consumer businesses rely more on innovative technologies to help retain customer loyalty, surpass consumer expectations and create competitive advantages in an everincreasing digital world.

As investments in new technology grow, so does the potential attack-surface, enabling cyber criminals to exploit weaknesses. This calls for a significant focus on cybersecurity, but our survey indicates that there is a general lack of basic cyber defence efforts among the surveyed consumer businesses.

What does the survey show?
The survey indicates that only about four out of ten of the surveyed consumer businesses have a cyber defence, with basic defence efforts being implemented in full or in part. This includes response plans, self-defence plans, cyber hygiene and cyber awareness training. 46% of the respondents state that they do not or only partly have a self-defence plan in place. Approximately half of the surveyed consumer businesses do not or only partly perform cyber hygiene practices. 53% of the respondents do not have a response plan in place – or only partly have one in place to some degree – that can be used if the business is attacked. Finally, 62% replied that they do not, or only to some degree, conduct regular awareness training. Only 16% of the respondents that have ranked their cyber defence seven or higher have fully implemented all four cyber defence efforts.

Deloitte's perspective
Based on the respondents' positive self-evaluations, an assumption would be that the majority have fully implemented the basic set of cyber defence efforts. Ou spondents ranking themselves seven or higher h ave fully implemented all four basic defence efforts. This supports the argument that several businesses might operate with a false sense of confidence in their cyber defence.

"I'm actually not sure that we've got a SOC response plan. We've several playbooks, but not a complete plan for everything".

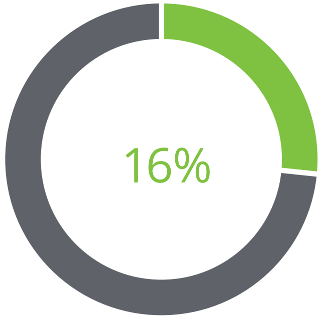
CISO of a large, Danish consumer business.

"We do have a response plan, but it isn't written down so I wouldn't be able to show it".

CIO of a large, Danish consumer business.

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.

Based on the findings of the survey, it therefore seems fair to conclude that there are bright spots in Danish consumer businesses when it comes to cybersecurity, but also quite some room for improvement. Luckily, there are plenty of low-hanging fruits that can be harvested relatively easy to strengthen the consumer businesses' cyber defence and resiliency. For instance, many organisations just need to operationalise the knowledge, plans or procedures that already exist within the organisation but have not yet been written down or systematised.



16% of the respondents that have ranked their cyber defence as seven or higher have fully implemented all four cyber defence efforts.

Deloitte.