Deloitte.

Energy, Resources & Industrials Cyber Survey

February 2021

Editorial

Businesses in the Danish ER&I sector are on a journey towards maturity in cyber security. Slowly but surely the matter is becoming an integral part of company mindsets. Although many security areas lack the necessary attention and shortcomings are easy to point out, Danish ER&I businesses have taken a giant leap towards cyber security within the past years.

In this survey, we investigate the Danish ER&I sectors' ability to respond to threats from the current cyber security landscape. Besides unique insights into the cyber security practices in the sector, our survey reveals three major trends:

The cyber security threat has increased significantly. There is an overwhelming consensus that cyber criminals are targeting Danish ER&I businesses with increasingly sophisticated strategies and resources, and COVID-19 has added fuel to the fire. However, our survey reveals that Danish ER&I businesses lack critical defense mechanisms to mitigate the consequences of an attack. Thus, many Danish ER&I businesses display incongruities between the perceived threat level and the strength of cyber defenses, leaving the door open for criminal breaches of crucial systems.

Cyber is climbing the agenda of top management. The increased threat level and the devastating ramifications of a successful attack have forced cyber security onto the boardroom agenda – but not yet as a top priority. Going forward, it is critical that leadership takes the time to receive regular input from IT security professionals. If not, decisions on budget, risk and security level are at risk of being underprioritized.

Suppliers pose the greatest security risk. Danish ER&I businesses must actively monitor countless threats to their systems. But the survey's data indicates that the biggest risk is presented by suppliers not closely connected to the organisation. Thus, outsourcing takes center stage as an area of concern, underscoring the need to apply security measures to the full value chain.

In summary, the cyber security efforts of Danish ER&I businesses leave ample room for improvement. But the progress shown by the sector lights way forward when upgrading the effort.

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

Kim Sclyter
Partner
+45 30 93 44 92
kschlyter@deloitte.dk

The increased cyber threat reveals cracked defences

There is a strong consensus among Danish businesses in the ER&I sectors that the cyber threat has been growing and Covid-19 has distorted the threat landscape and added fuel to the fire. Now, organisations need to take action or risk falling victim to inevitable attacks.

But are they ready? The past few years have seen Danish ER&I businesses facing an increase in the frequency and intensity of phishing and ransomware attacks. This development builds on the general trend of cyber threat escalation that we have seen during the same period. The question is: Can the cyber defences implemented by the businesses surveyed keep up with the growing cyber threat?

What does the survey show?
79% of respondents have experienced an increase or a significant increase in the cyber threat during the past two years. 21% believe the threat has stayed the same. None believe in a decrease. In addition, 34% of respondents believe Covid-19 has resulted in an increased cyber threat to their businesses.

The most popular pre-emptive measure taken by the surveyed businesses is a self-defence plan. 86% have completely or partly introduced such a measure. However, it is worth noting that 62% of the surveyed businesses do not operate with a fully actionable response plan in case of an attack.

Deloitte's perspective
It is highly surprising that 37% of Danish ER&I businesses do not have a self-defence plan ready in case of an attack. In an environment of critical increase in the cyber threat, we can only appeal to all businesses to prepare themselves as soon as possible.

> "We test it (cyber defences) on a regular basis and run different kinds of drills. We could, of course, do even more, but we have to take time, money and output into consideration".
>
> *Cyber Security Business Architect, large Danish ER&I business.*

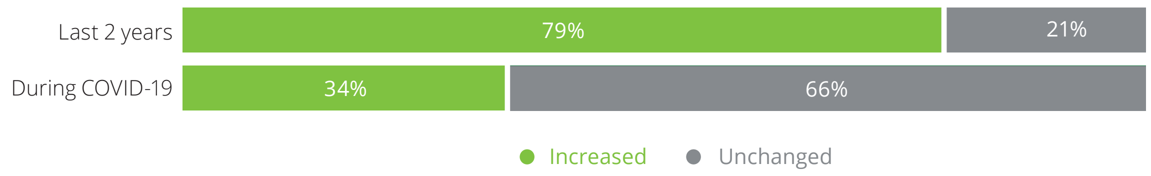
While it is positive to see that a big majority perceive the threat level to have increased during the past two years, the fact that 21% of the respondents have not noticed a change in the threat level during that time, and that 66% have not experienced an increase during Covid-19, indicate that it is necessary to revisit the cyber threat assessment for some Danish businesses in the ER&I sectors.

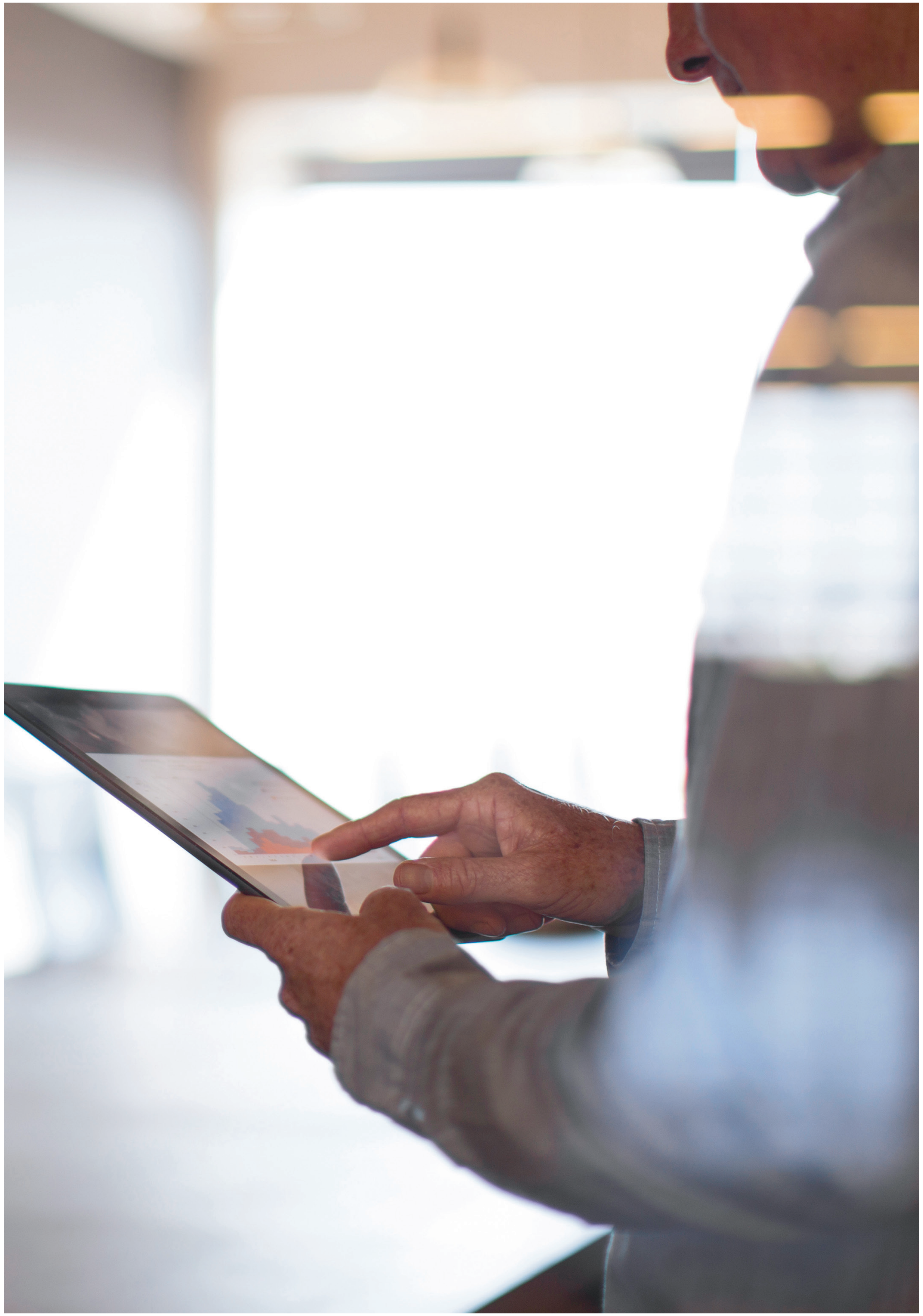
According to Deloitte's cyber experts, building a resilient cyber defence begins with a detailed threat assessment, weighing the likelihood of different threats and embedding prioritised security measures in a proportionate response. Altogether, this should form the strategy used throughout the organisation.

Based on the survey, it can be concluded that some Danish ER&I businesses retain a mismatch between threat level and cyber defence, thereby perpetuating a potent security risk. In the effort to stay secure during a time of heightened threat, it is crucial to free up the needed resources and create access to sufficient data. This provides the insight needed to build a realistic understanding of how the threat landscape is evolving. Not having a realistic understanding of such developments renders mitigation of the threat nearly impossible.

> "In 2016-2018 we took a huge leap from almost no security to getting something started. Today we are still feeling the positive effects of that effort".
>
> *CISO, large Danish ER&I business.*

How has the cyber threat against your organization in your view developed?





Mixed commitment from top management

A surge in the general cyber threat level combined with several critical cyber attacks on major Danish businesses have finally put cyber security on the leadership and boardroom agenda of Danish ER&I businesses. But commitment has been mixed.

Top management at Danish ER&I businesses are clearly discussing cyber security. But although the survey reveals positive tendencies, there is still ample room for improvement.

What does the survey show?

According to 30% of the businesses surveyed, cyber security is on the leadership agenda weekly or monthly. 34% discuss cyber security in the boardroom on a quarterly basis, 8% on bi-annual basis, while 27% indicate that cyber security has the leadership's attention once a year or less frequently.

Deloitte's perspective

On a positive note, the survey shows that cyber security is taken seriously in some boardrooms and by some top management teams within the sectors. The increased threat level and the potential ramifications of a successful attack have forced cyber security onto the agenda.

"We have discussed the cyber threat at board level for some years. Cyber risk is actually the only IT risk at board level".

CISO, large Danish ER&I business.

But the fact that 27% of the respondents indicated that cyber security is not on the management agenda more than once a year or even less frequently poses a significant threat to those businesses. It is critical that IT managers and CISOs inform the leadership regularly. If not, it can be difficult for top management to make informed decisions on budget, risk and security level. Top management must thus take time to get directly involved in strategic cyber initiatives.

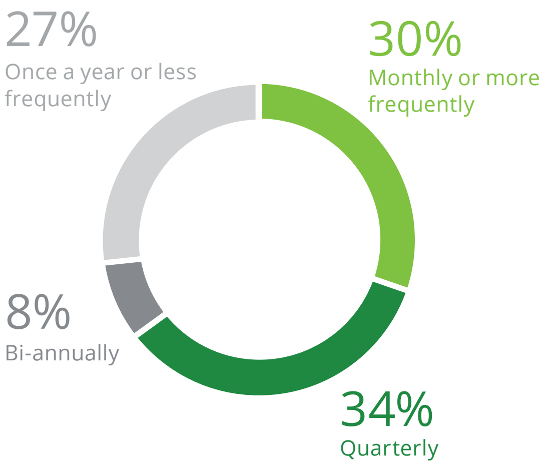
"We actually do have management that is quite committed to having this under control, and I am pretty surprised about how big the commitment is".

Cyber Security Business Architect, large Danish ER&I business.

The consensus is that the cyber threat is surging. Therefore, every leadership team in each of the sectors should have cyber security at the top of their agenda. It is vital to meet regularly with expert-level employees to assess and discuss the cyber threat. The surge in cyber attacks during Covid-19 is a good example why.

After all, it is the responsibility of management to ensure the creation of an effective strategy for when worst-case scenarios occur. The survey, however, seems to indicate that top-level discussions on cyber threats are not as frequent as recommended.

How often is cyber security on the top leadership's agenda?



"Typically, decisions are not taken by top management. It is done at the levels below".

CISO, large Danish ER&I business.

Sustainability agenda eases talent access

Most businesses have a hard time gaining access to top IT talent. Danish ER&I businesses are no exception. But the popularity of the sustainability agenda seems to provide an edge.

Like many others, Danish ER&I businesses are in the market for the brightest minds within cyber security. Due to the small talent pool in Denmark, many of the businesses employ IT talent on a global basis and accept remote work to some degree. This relieves the recruitment pressure.

But even so, competition for global talent among the surveyed businesses is fierce and many have a hard time satisfying their needs. However, it appears that most businesses in the survey are not challenged to the extreme. Some respondents believe this is due to the attractiveness of the sustainability agenda, which many businesses in the sectors tap into.

> "We have a very good profile right now. People think that it is exciting to work for an environmentally minded organisation. So, we attract people with a different ambition than just money".

Security Architect, large Danish ER&I business.

What does the survey show?
12% of respondents believe it is easy or very easy to attract cyber talent. 14% believe it is difficult or very difficult. A majority of 74% believe that it is neither difficult nor easy. 33% believe retaining talent is easy or very easy. Developing talent is considered easy or very easy by 41% of respondents.

Deloitte's perspective
A few years ago, the Danish pool of IT talent was almost non-existent. Today, however, as the focus has increased and educational institutions have adapted, the talent pool has become bigger and Danish businesses in general have an easier time attracting, retaining and developing qualified Danish talent. At the same time, global interconnectedness – sped up by Covid-19 – has made it easier to pick and choose from the global pool of IT talent.

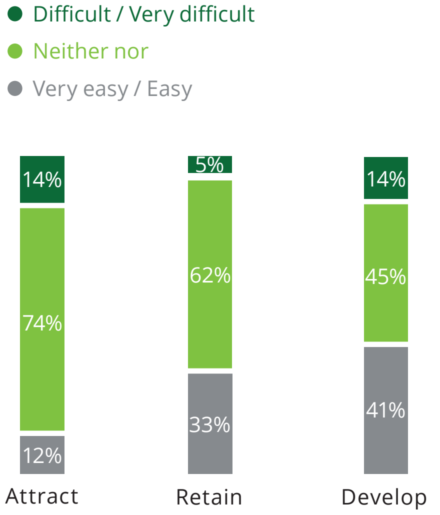
It is positive to see that 86% of the surveyed businesses do not regard talent attraction in the cyber security realm as an obstacle. Danish ER&I businesses have an innate focus on technical expertise within production. It is possible that this arena of technical expertise spills over into the IT department, creating an ideal environment for technical sparring. It is also likely that the sustainability agenda, which many of the businesses are tapping into, gives them an edge when recruiting talent.

Compared to many other sectors competing for cyber talent, large Danish ER&I businesses can consider themselves fortunate – for now. The optimistic nature of the responses could well be the result of the fact that many of the surveyed businesses have not yet entered a mature phase of IT recruitment. Thus, they will – sooner or later – reach the same limits of cyber recruitment that so many other sectors struggle with.

> "It is not realistic to find someone in Denmark who can do this to the extent we need. We have to find a way in between".

Cyber Security Business Architect, large Danish ER&I business.

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



Cyber security is neglected as green technologies advance

The ER&I sectors are subject to extreme change due to global climate objectives. Will there be room for cyber security in an era of rapid green transformation?

Nowadays, ER&I businesses are being pushed to carry out an unprecedented transformation for the sake of sustainability. New technologies must constantly be developed and put into use in order to limit emissions and comply with regulations. Nonetheless, responses from the survey shows that for many ER&I businesses, the technology related to climate transformation is not considered to be relevant to the cyber security agenda**.**

What does the survey show?

In general, the surveyed businesses remark that climate transformation and cyber security do not go hand in hand. The two fields appear to be completely separated. This way of thinking seems to be reflected in the dominant approach to security by design in which 53% of businesses do not take cyber security into account before the development phase.

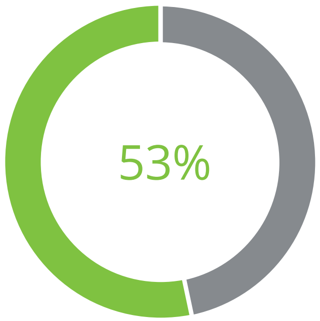
Deloitte's perspective

There is nearly a 50/50 split between businesses that adhere to security by design and businesses that do not. This indicates that there is still a long way to go before all products are secure from the get-go.

The climate transformation urges industrial energy companies all over the world to invent new technologies and implement them at record speed. But when creating a new product, it is important to build security into its foundation. Most green technologies are tied to the Internet in some way or another. In order to reduce the carbon footprint, systems must be modernised and digitalised. This makes them more efficient but also vulnerable to attacks.

> "Our climate transformation and cyber security have nothing to do with each other. Cyber security is just a part of our IT".
>
> *Respondent Cyber Survey, Danish ER&I Business.*

If these technologies are not secure by design, the efficiency of any later security measures cannot be guaranteed, rendering the technology detrimental to both security and climate transformation. Therefore, security by design is crucial to the development of all new technologies. Simply put, security by design needs to permeate the whole organisation and especially the agenda of climate transformation.



Think about last time your company developed a digital solution (e.g. website, digital product, booking system, app etc.). When in the development process was cyber security taken into account?

● Before development

● During / after development or not considered

Outside suppliers pose the greatest threat

While the general confidence in cyber resilience is high, outside suppliers pose a threat to many Danish businesses in the ER&I sectors.

It is beneficial for all businesses to become interconnected, but there are also drawbacks. The survey reminds us that the security of supply chains is always decided by the weakest link. Thus, Danish ER&I businesses struggle to maintain cyber security due to lax approaches by outside suppliers.

What does the survey show?
Overall, when it comes to cyber attacks, the surveyed businesses consider themselves highly resilient. 83% believe they are resilient to a high degree when handling customer data. 68% indicate the same level of cyber security when using cloud services. 65% believe the level of security is high when cooperating with close partners and suppliers. However, it is clear that less integrated outside suppliers pose the greatest threat. In this domain, only 37% of respondents believe they are resilient to a high degree.

Deloitte's perspective
It is promising to see that the increased focus on the cyber threat has led to an unprecedented awareness of cyber resiliency. To some extent, it is positive that businesses rate their security with confidence in many areas. However, a high level of confidence can also be a double-edged sword.

A more alarming conclusion is that 63% of the respondents feel they are not highly secure in areas of the supply chain that involve business partners and suppliers that are not closely connected to the organisation. This is a trend also seen in the consumer sector.

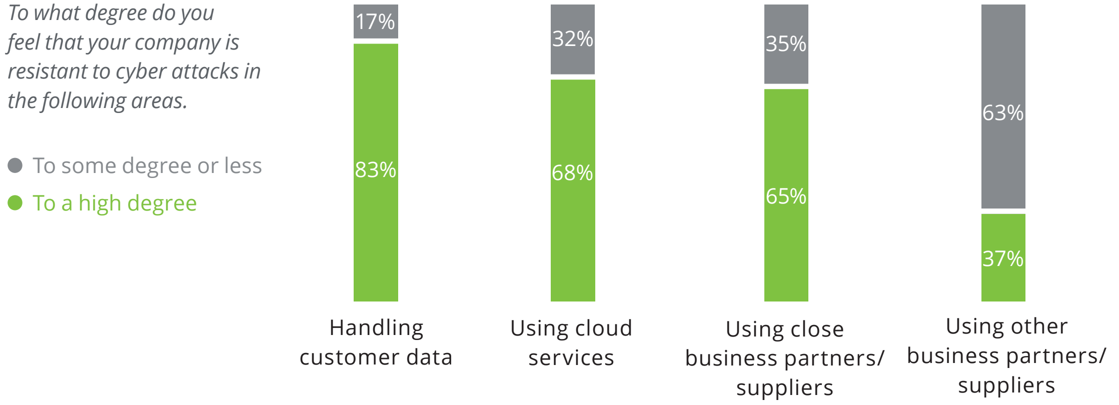
> "We try to get control over our suppliers, but it is difficult because we have so many. But this is something we need to be better at".
>
> *Cyber Security Business Architect, large Danish ER&I business.*

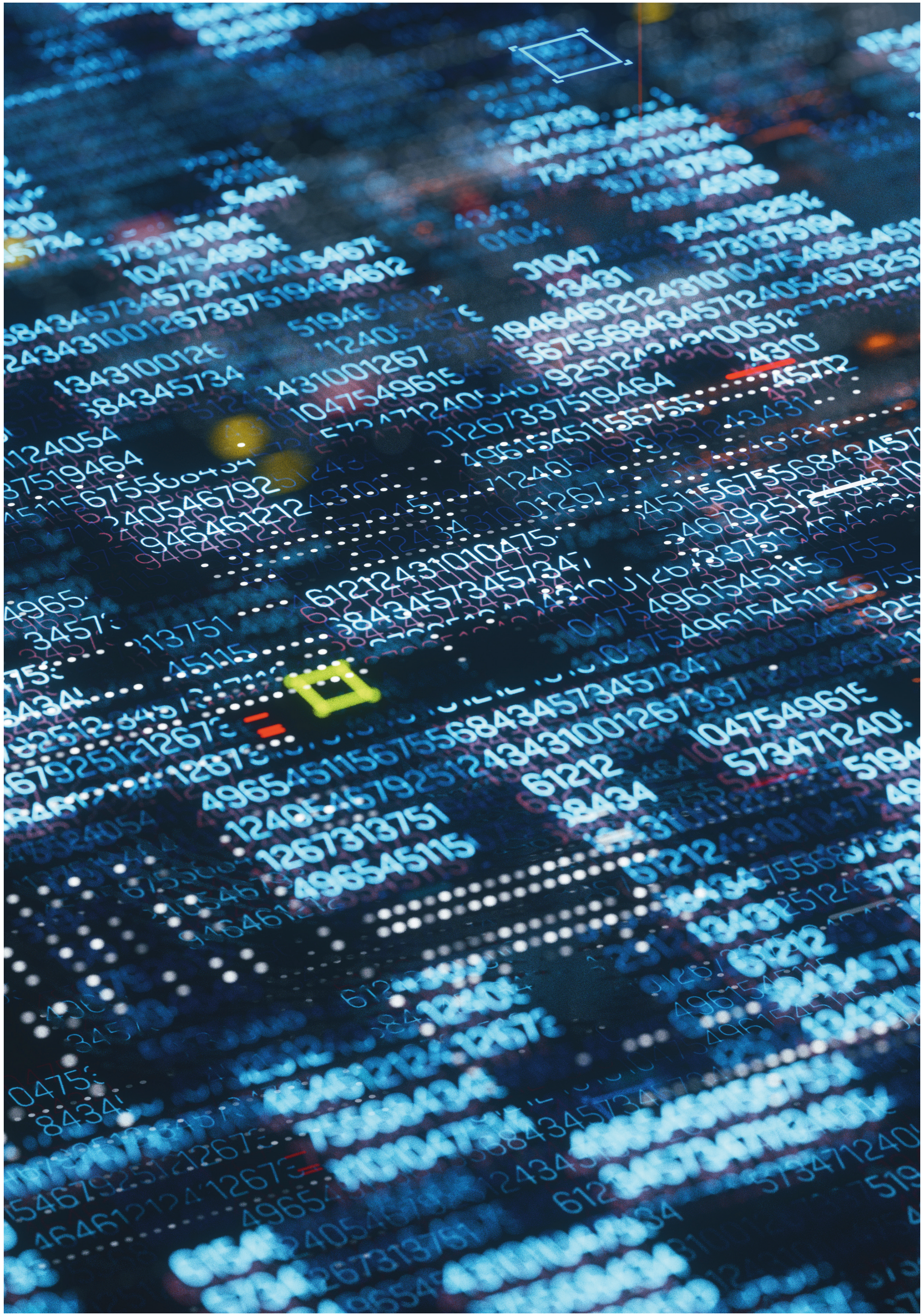
This causes concern, particularly as many businesses are currently experiencing an increase in attacks that target the supply chain. By attacking the weakest links in the chain, attackers can use the suppliers as entry points to the organisation's main systems. These attacks can be detrimental to any organisation.

In conclusion, it is apparent that businesses in the Danish ER&I sectors are in a maturing phase of cyber security – one in which outsourcing becomes an area of concern. Large ER&I businesses need to apply security to the full value chain in order to be secure. If not, engaging with outside suppliers can result in loss of control.

> "In recent years, we have become much, much better at making demands on our partners on how to document and protect their access to our environments".
>
> *Security Architect, large Danish ER&I business.*

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





Reflecting on the ideal cyber defence

In an ideal world, cyber security would be deeply rooted in every organisation and permeate every action and decision.

Cyber experts in the Danish ER&I sectors agree that the threat of cyber attacks is increasing. In many areas, they also see themselves as highly resilient to attacks. But, in their own view, how well are businesses performing overall?

What does the survey show?
When asked to which degree they have obtained the ideal cyber defence, 9% of the surveyed businesses perceived themselves as highly secure, ranking themselves at nine or even ten on the security spectrum. 18% rank themselves an 8. 29% rank their security performance at a seven. 30% rank themselves at five or below

Deloitte's perspective
In the section on cyber resiliency we saw a high degree of confidence within Danish ER&I businesses. However, when it comes to the overall perception of performance, that confidence seems to dip.

It is worrying that 30% of the surveyed businesses rate themselves in the lower half of the spectrum. This means there is plenty of room for improvement. However, it can also be interpreted as promising that a majority of 56% rate themselves seven or higher.

There is no doubt, however, that the consumer demand for cyber security is increasing. Cyber has already become an essential part of modern governance and compliance and soon unsafe products and companies will lose to safer competitors. Thus, security is necessary in order to be taken seriously as a partner or supplier.

It is an important leadership task to take this responsibility seriously and keep in mind that there is no commercial performance worth achieving if cyber security is not obtained first.

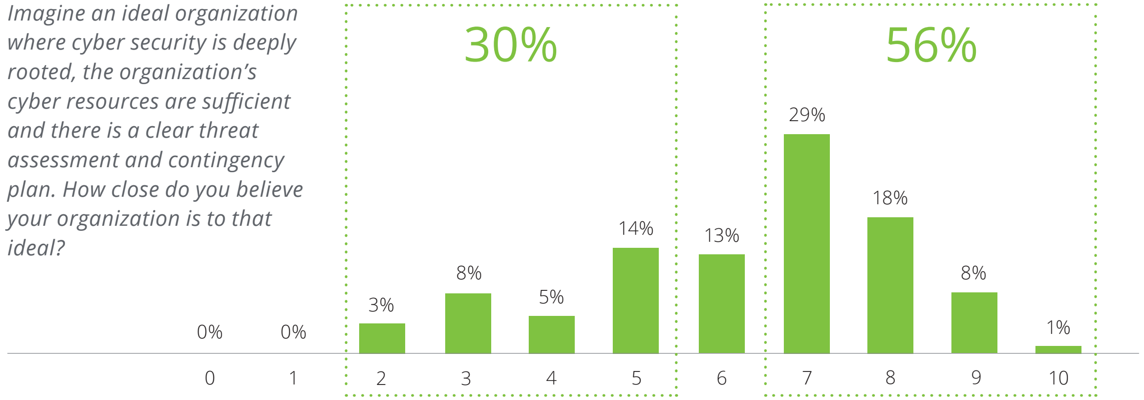
> "We haven't been involved in any major cases. But whether it's because we're resistant or because there's just no one who's broken in yet, we don't know".

Cyber Security Business Architect, large Danish ER&I business.

> "We are still in the beginning of all this. So, I would say that it is pure luck that we have not been attacked yet".

Security Architect, large Danish ER&I business.

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



Deloitte.