Deloitte.

Hacks me, hacks me not…

Cybersecurity is the
Achilles heel of Danish businesses

Cyber Risk Landscape Report 2019

Foreword

Cyberattacks pose a significant threat to Danish businesses today. As a society, we thrive on our knowledge enterprises, our coveted trade secrets, and modern research divisions that place us on the cutting edge of many industries and sectors. The Danish society is built on a high degree of trust and connectivity. Denmark is also one of the most digitalised countries in the world. All of this makes us a popular target for adversaries.

In this year's survey we fundamentally sought to understand the level of awareness of the prevalent cyber threat to our society and businesses. We also wanted to measure our businesses' preparedness against a plausible electronic disaster. Our key conclusion is that – even with the well-advertised cyber disasters less than two years ago – Danish businesses remain trusting and over-confident in the cyber arms race. Cybersecurity also remains to be the mythical beast of IT with little understanding amongst the executives and presence at the top.

This is a wakeup call that we all need to heed. I cannot stress enough for this picture to change. We would like to draw your attention to three key takeaways. First, we need to continue educating our leaders on cybersecurity but also give our cyber leaders an independent voice and a seat at the table.

Second, we need to find better ways to quantify and justify cybersecurity investment and align our language to the business. In this report, we outline several ways to do so. Third, planning and testing makes champions. We encourage frequent and a variety of fire drills to keep you vigilant and prepared – for that rainy day.

We hope you find the insights from this report interesting. Please do not hesitate to reach out to us for further conversations.

Serdar Cabuk, Ph.D.
Partner, Nordic Cyber Leader
+45 30 93 50 70
scabuk@deloitte.dk

Chapter One

Cyber at the top

Majority of the Danish firms appointed a designated cybersecurity leader.

A quarter briefs their Board or C-suite on cybersecurity once a year or not at all.

Winning the Boards' hearts and minds

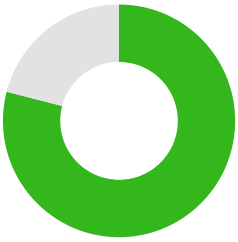
Financial and cybercrime remain the dominant motives for the adversaries in the Danish market.

Cyber espionage will be a particularly critical threat in the coming years. Cyber threats are constantly evolving. Even so, cybersecurity still does not attract the attention that it deserves at the top.

What we heard

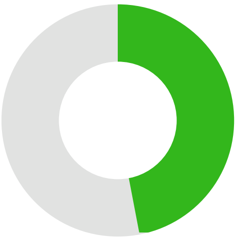
A promising 79 per cent of the Danish firms appointed a designated leader for cybersecurity, for example a CISO, Chief Information Security Officer or an IT Security Manager. Only 47 per cent of these leaders are members of the executive management team; 55 per cent think they ought to be.

A quarter of these companies' executives have never been briefed on cybersecurity or have only been briefed once a year. Over 30 per cent did not know whether the information provided was adequate for the C-suite.



79 %

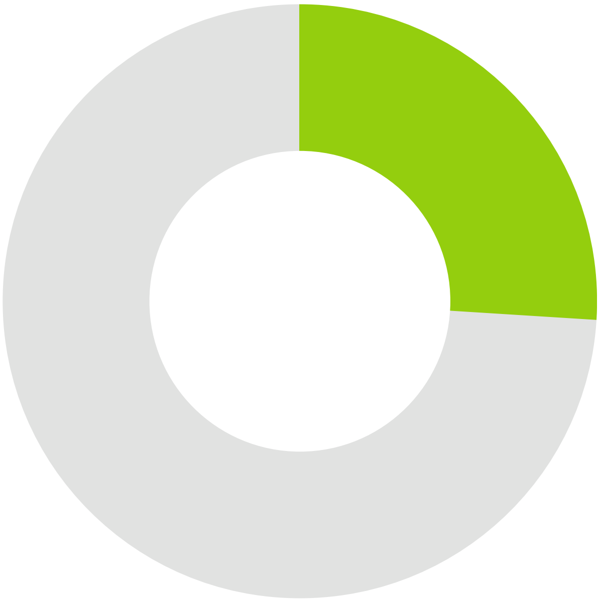
have appointed a designated cybersecurity leader



But only

47 %

of these leaders are members of the Executive team



26 %

of the executives are either never or rarely briefed about the cybersecurity status

What we think

It is positive that the majority of the Danish firms have appointed a designated cybersecurity leader. This is a considerable improvement from a decade ago when such a role did not exist. Representation at the top, however, is still problematic. Surveys continue to rank cyberattacks as one of the top risks to Danish businesses today. This should naturally lead to cybersecurity becoming a prioritised item on the executive agenda. According to the survey data, this is not yet the case.

One reason could be that cybersecurity is still considered as an IT problem. In contrast, recent cyberattacks showed that it is not IT but the entire business that is impacted by a successful attack. Ironically, even within IT, priorities of the CIO can somewhat conflict with those of the cybersecurity leader and the CIO might prioritise new capabilities over costly security measures.

It is challenging for the C-suite to have a good grasp of the cybersecurity issues – especially if they do not receive frequent, high quality briefings. Failing that, these leaders will have a false sense of security that is possibly not aligned with their organisations' risk appetite.

Executives in certain companies – e.g. those deemed as critical infrastructure – should play a key role in protecting their organisations against cyberattacks. Regular briefings are one way to do so; a better way is to educate them on cybersecurity so that they can take informed decisions in managing cyber risks. For others, we recommend cybersecurity briefings at a minimum on a quarterly basis.

What you should take away from this

Brief your Board and C-suite on cybersecurity but not as a tick-box exercise

A good briefing comprises of operational and threat data linked to business risks. These briefings should be at least quarterly but also when there are major changes in the organisation (e.g. a digital transformation program) or a major shift in the external threat landscape (e.g. a new threat actor or a major attack vector).

Train and test your Board and C-suite on cybersecurity and business impacts

Briefings alone are not sufficient. Companies should organise regular training tailored to the Boards and C-suite on specific cyber risks aligned to the business KPIs. The objective is to enable these leaders to make the appropriate investment on cybersecurity in-line with the company's risk appetite.

Provide your cybersecurity leader independent investment and a seat at the table

Several companies have started achieving this by placing the CISO outside of the IT organisation – e.g. as a direct report to the CRO or COO – or establishing a direct or indirect reporting line to the Board of Directors or the CEO. The latter setup is still fairly rare.

In all cases, the cyber leader should be sufficiently independent from IT and the CIO act as a stop-gap and take risk-based decisions and be sufficiently independent from the risk & compliance organisation so that security does not become a check-box exercise.

Investing in cybersecurity

When determining the cybersecurity budget, an organisation must first decide the level of cyber risks it is willing to tolerate, e.g. through a defined risk appetite. Naturally, setting a low tolerance for cyber risks requires higher investment in cybersecurity.

This needs to be a quantified assessment; relying on your gut feeling – when it comes to cybersecurity – can be expensive.

What we heard
In our survey, more than 60 per cent of the respondents believe that their organisations have sufficient budget for a cybersecurity program. Over 30 per cent either do not know or are undecided. In fact, over 42 per cent are either satisfied with their current level of investment or confident that they can manage for less.

Unsurprisingly, 40 per cent of the businesses that experienced at least one cyberattack during the past year requested an increase in their cybersecurity budget.

61%

think their budget for cybersecurity is sufficient

42 %

are either satisfied or think they can manage for less

40 %

requested a larger cybersecurity budget after experiencing a cyberattack

What we think
These results are surprising for several reasons. First, cybersecurity is generally an under-invested and under-regulated area. The issue has recently further deepened with digitisation across the industries, increased adoption of Cloud and explosion of data. Second, Denmark is ranked as the fourth most vulnerable country to cyberattacks. This does not align with the level of confidence in cybersecurity investment.

Sadly, the subsequent question shows that a successful cyberattack is still the most persuasive argument to unlock investment in cybersecurity. Organisations spend significantly more on cybersecurity after a successful attack; akin to spending on vaccines skyrocketing following a flu pandemic.

We believe that the underlying reasons for such over-confidence – and potentially false sense of security – are three-fold. First, our survey covered a large number of correspondents in the IT organisation, who are – in our experience – over-confident in their level of security whilst they focus on service availability and performance. We recognise that IT transformation and other business-driven topics may rank higher on the investment agenda than cybersecurity. We also believe that cybersecurity should be an intrinsic part of such transformation.

In Denmark, cybersecurity is not yet fully embedded in IT and business transformation programs. We see this trend in more mature markets such as the UK or the U.S. where security is seen as a major enabler of business, e.g. by convincing consumers to use digital products, moving more workloads to the Cloud securely or enabling data use by preserving security and privacy.

What you should take away from this

Start by finding out your current cybersecurity investment across the organisation

One way to determine whether you invested on cybersecurity sufficiently is to compare your cybersecurity budget to your overall IT spend. In our experience, cybersecurity investment varies between 8 to 13 per cent of the IT budget.

Collect all requirements from compliance, risk and change programs for cybersecurity

Meeting regulatory requirements and closing audit findings continue to be key for your cybersecurity investment case. Your case should also include cybersecurity elements in your change programs – especially those that involve significant technology investment (e.g. Cloud), complex regulatory frameworks (e.g. GDPR, PSD2) or major business transformation (e.g. digitalisation).

Use business objectives and KPIs to drive and defend cybersecurity investment

In addition to audit, risk and compliance requirements, you should align your cybersecurity budget to your business objectives. Two examples of such objectives are (1) revenue protection, e.g. by improving operational resiliency and "keeping the lights on" and (2) accelerating IT or business transformation, e.g. by alleviating any security concerns of your target audience – consumers and regulators.

Mature organisations use "impact tolerance" as a quantifiable metric for cyber resiliency

Impact tolerance for cybersecurity is the ability of an organisation to withstand or recover from a severe but plausible cyberattack. An example is to "service 100% of your online customers within X days after a severe cyberattack". Setting a quantifiable target is a challenging task; but it will be more convincing for your Board and regulators.

Second, quantifying cybersecurity investment has been problematic as it spans across multiple IT and business domains – and relies on quantification of the underlying risks. For example, companies have been struggling historically to put a premium on reputation risks.

Third, these results may actually be a reflection of the common misbelief that the current investment (e.g. on security products) buys the companies "more security" than it is in reality.

The arms race in cyber skills

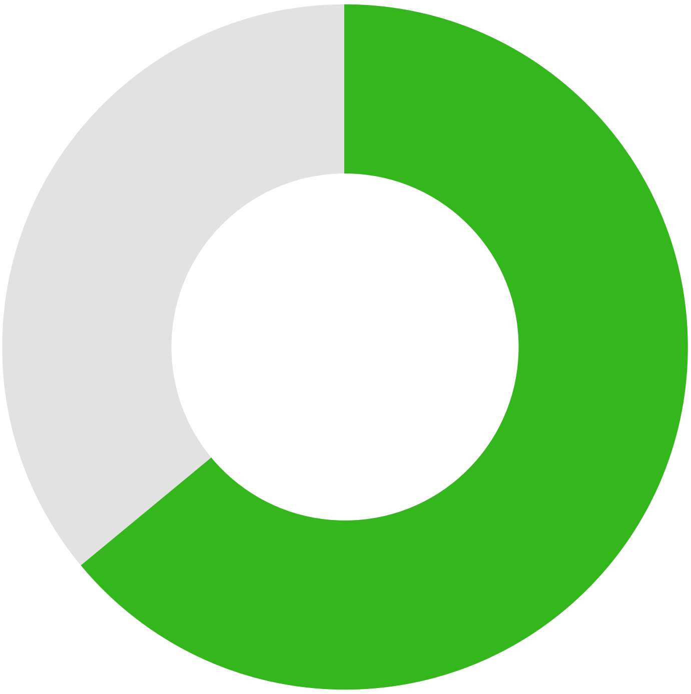
A common issue for any Danish business today is to attract and retain the right talents and skills to make sure that the organisation is prepared for a digital future.

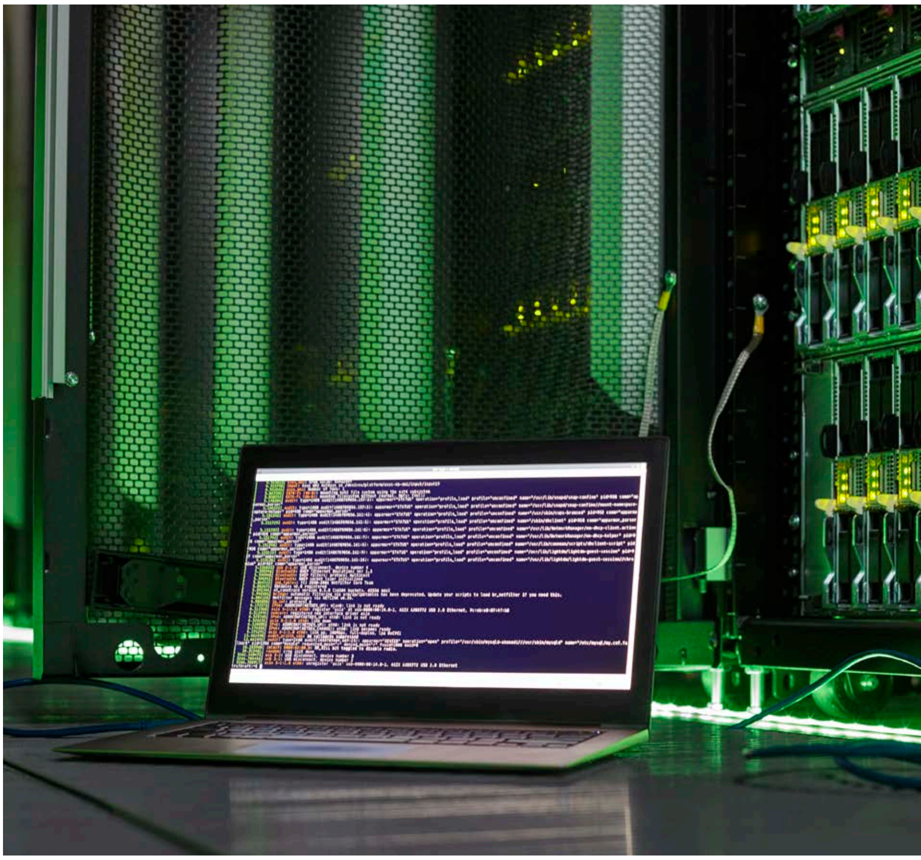
With the increasing sophistication of the cyberattacks and the actors involved – such as nation states – this is more essential for the cybersecurity field than ever.

64 %

are comfortable with their organisations' cyber skills

What we heard
Previous studies have consistently suggested that there is a significant talent gap within the field of cybersecurity. In stark contrast, our survey shows that over 64 per cent of the respondents are comfortable with their organisations' cyber skills.





What we think

In our view, the Danish firms are over-confident in the assessment of their cyber skills. This is in-line with our interpretations in Section 2; a similar percentage believes that their investment in cybersecurity is sufficient. We urge the firms to independently assess their skills before they are tested in a real cyberattack situation.

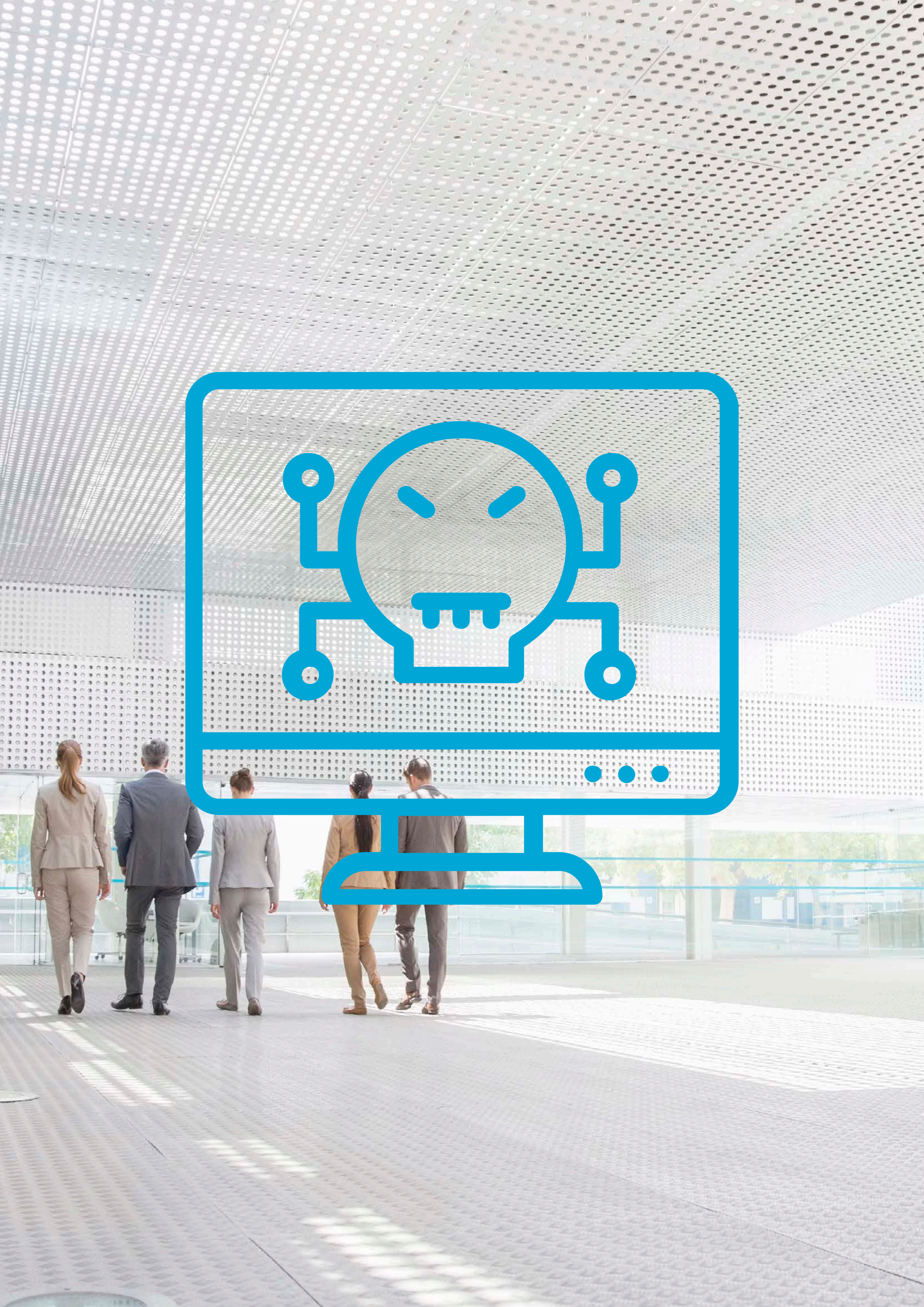
What you should take away from this

Invest in attracting cyber skills as well as retaining them

Cybersecurity is a "sellers' market" with several companies requiring these skills drawn from a limited pool. Creating an attractive cyber-culture and retaining such talent requires continuous investment in skills, people and training.

Train your technical, business and general staff on cyber

Training is a key element in filling the skills gap. It is important to offer extensive training to your most technical staff, the forefront of your cyber defence, using new and innovative training techniques such as gamification. Operational roles in IT can also provide valuable skills to your cybersecurity workforce to gain real life experience through shadowing or staff rotation.



Chapter Two

Ready for a cyberattack?

Plan, test, respond — repeat

Danish firms cut corners when it comes to cyber incident management.

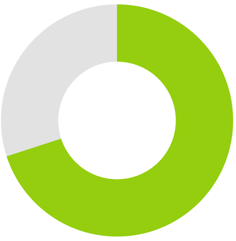
Under attack

Organisations that are able to detect the early stages of a cyberattack, e.g. during reconnaissance, can naturally initiate a more effective response and reduce response and recovery times.

The ability to detect a sophisticated cyberattack is the key first step in reducing the potential damages to your business.

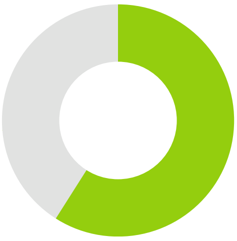
What we heard
Our survey shows that 46 per cent of the respondents experienced at least one cyberattack in the past 12 months. 38 per cent have not experienced any attacks. These figures are lower than the average figures reported in recent studies.

A staggering 70 per cent of our respondents are also convinced that they can detect a sophisticated cyberattack. Majority of the CIOs agree. About 59 per cent are using cyber threat intelligence programs to anticipate future cyberattacks.



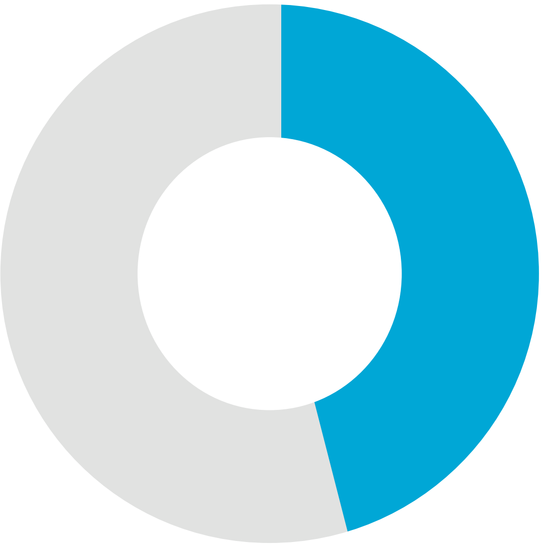
70 %

are convinced they can detect a sophisticated cyberattack



59 %

have a cyber threat intelligence programme



46 %

have experienced at least one cyberattack in the past year

What we think

Cyberattacks occur all the time. Many go unnoticed – either due to the lack of capability to detect them or the adversary taking extra steps to keep the attack quiet for maximum gain.

In our experience, it is difficult for organisations to detect cyberattacks. In fact, several studies report that the majority of cyber breaches are discovered by external parties. It also takes a substantial amount of time to do so. One contributing factor is the cyber skills gap in organisations fighting against sophisticated adversaries. Another factor is the inability to collect, collate and extract valuable security information to produce actionable intelligence on attacks.

We also believe that the number of cyberattacks is generally under-reported. It is a widely accepted notion that it is not a question of if but when you a cyberattack will take place.

The discrepancy between the survey results and several studies on the subject is alarming. One way to test whether you can actually detect cyberattacks is to run unannounced and regular security tests of different forms – varying from traditional penetration tests to Red Teaming exercises running under-cover. Another way to verify this is to actually find out what security monitoring solutions are in place and which systems you are actively monitoring. If you cannot see what is going on in your organisation, you will not detect a sophisticated attack – until the damage is done; sometimes not even then if the adversary wants to keep it quiet.

What you should take away from this

Detecting cyberattacks require the right blend of people and technology capabilities

Without data, your cyber teams will not identify an attack against your network and key systems. Too much data will overwhelm them to identify what is important. The balance is when you employ the right technology to collect and interpret data into actionable information. This will then be consumed by your cyber teams in identifying and responding to cyberattacks.

Run regular security tests and Red Team exercises to check your detection capability

Security tests are useful to identify vulnerabilities. They are also useful to assess the ability and efficacy of your detection capabilities – i.e. whether you can detect an attack, and if so, how quickly. These security tests should run under the radar and use techniques to hide the attack. The results will provide undisputable evidence on your detection abilities.

Enhance your reactive detection capabilities with proactive threat intelligence

A good threat intelligence program will enable you to anticipate relevant cyber threats to your organisation and – in most mature organisations – take proactive measures before a likely threat is realised (e.g. emergency patching a vulnerability outside maintenance windows before an imminent attack).

Planning and testing make champions

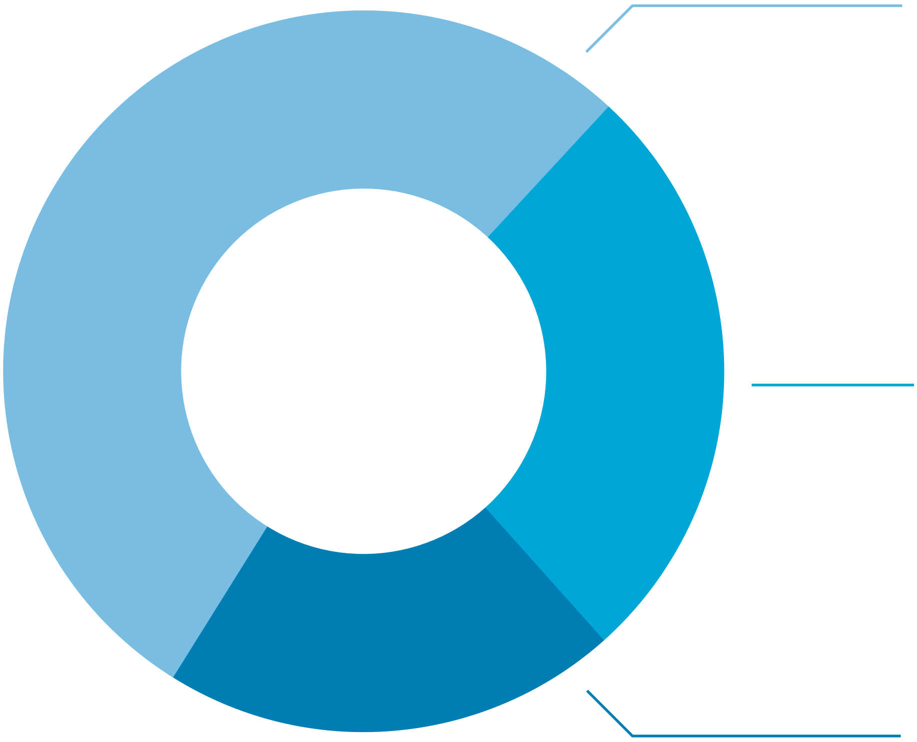
Cyberattacks in the last two years have shown that small and large organisations alike can be victimised. It is vital to forward plan your security incident response and regularly test it.

If you wait long enough, an actual cyberattack will test your plans – which may be too late.

What we heard
A clear majority of the organisations that we surveyed have an incident response plan for cybersecurity. They also have a clear communication strategy in the event of a significant attack.

The results are less impressive when it comes to testing cyber incident response plans. Only 53 per cent of our respondents tested their incident response plans in the last six months. 27 per cent reported no such tests and 20 per cent did not know.

During the last six months



53 %

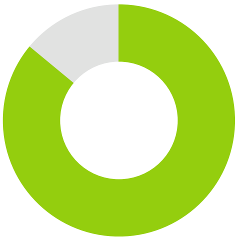
have tested their incident response plans

27 %

did not make a cybertest

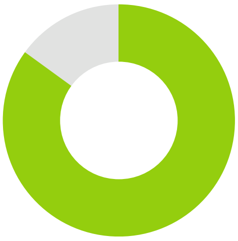
20 %

do not know



86 %

have a clear communication strategy in case of an attack



85 %

have an incident response plan

What we think

Danish businesses take an inconsistent approach to being prepared for a cyberattack. Whilst most agree to have a plan in the first place, there is disagreement on testing the viability of these plans.

Current and upcoming cybersecurity regulation in Denmark will likely change this behaviour. For example, GDPR imposes a 72-hour window to report data breaches to the national information commissioner. This not only requires having a plan but also testing it (along with your suppliers) to be able to meet the timeline.

The NIS directive has a similar requirement for incident response for organisations that are part of the Danish critical infrastructure. In our experience, similar requirements will also apply eventually to the companies outside of this group.

Whether required by the authorities or regulatory bodies, cybersecurity tests provide plenty of useful information about the efficacy of your capabilities (people, technology and controls) in a cyberattack scenario. It can also help demonstrate the value of your cybersecurity investment to the Board and C-suite.

What you should take away from this

Create and maintain an incident response plan for cybersecurity

A good plan will outline several scenarios involving cyber incidents and detailed steps to evaluate and respond to them. The plan should also clearly identify the roles and responsibilities for security incident management, linkage with broader IT incident response plans and crisis management in the event of a major incident.

Regularly test incident response plans using a variety of methods

Two such methods involve the traditional table-top exercises to walk through the plan and a full simulation exercise that simulates an actual cyberattack. At a minimum, we recommend an annual simulation/war-gaming exercise to test your ability to respond to cyber incidents. This involves the entire business, including the executives, communications, public relations, and deployment of Red and Blue teams.

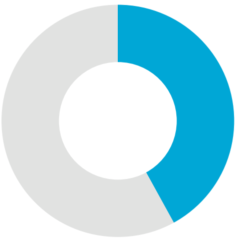
Back in business in no time

Danish business leaders believe that their organisations can recover from a significant attack in the blink of an eye. The recent successful attacks tell a different story.

What we heard

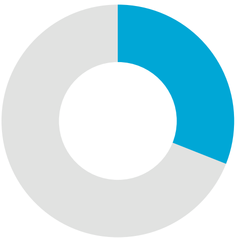
Our survey shows that half of the respondents believe their organisations can recover from a significant attack and return to business as usual within a couple of days. More than a third believe that it will take them a day. These are ambitious targets for companies in any industry – even for those deemed as critical infrastructure.

Small organisations are more optimistic. 42 per cent of the organisations with less than 500 employees believe they can recover from an attack within one day. Only 31 per cent with more than 1,000 employees share this view.



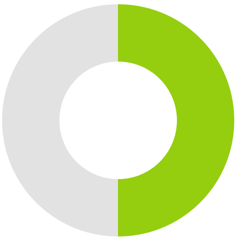
42 %

of organisations with less than 500 employees believe they can recover within one day



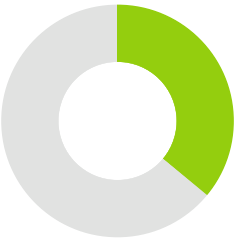
31%

with more than 1,000 employees share this conviction



50 %

think they can recover and return to business within a few days



36 %

believe that it will only take one day to fully recover

What we think

We believe that our respondents are overly optimistic on the impact of a significant cyberattack to their businesses. 'Business as usual' and 'significant cyberattacks' are subjective in nature. However, returning to normal operations within 24 hours following a severe attack (e.g. full service outage with data corruption) is a challenging task.

In fact, damages caused to major corporations during the NotPetya and WannaCry cyberattacks showed that a significant attack from a previously

unknown adversary can take months to contain and recover fully.

What you should take away from this

Embed cybersecurity into your business continuity plan

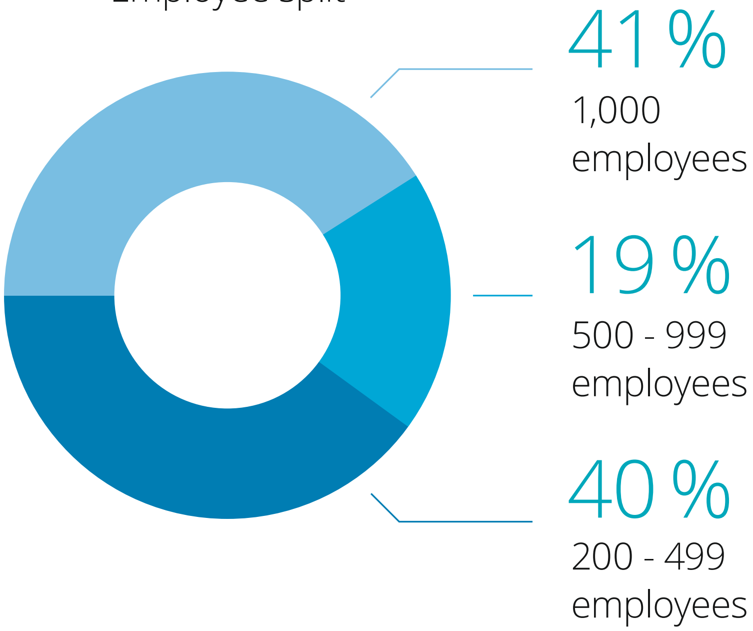
A cyberattack is now a severe but plausible scenario that should feature in your business impact analysis. To do so, you first need to identify your critical assets that are vulnerable to a cyberattack (e.g. your online platform). Next, you should define a tolerance level that you are prepared to accept given the cyberattack scenario – ultimately coming up with a quantifiable target (e.g. servicing 100% of customers within two days following a successful attack). This requires a thorough analysis followed by testing to ensure that you can remain within tolerance.

Security harden your critical IT assets

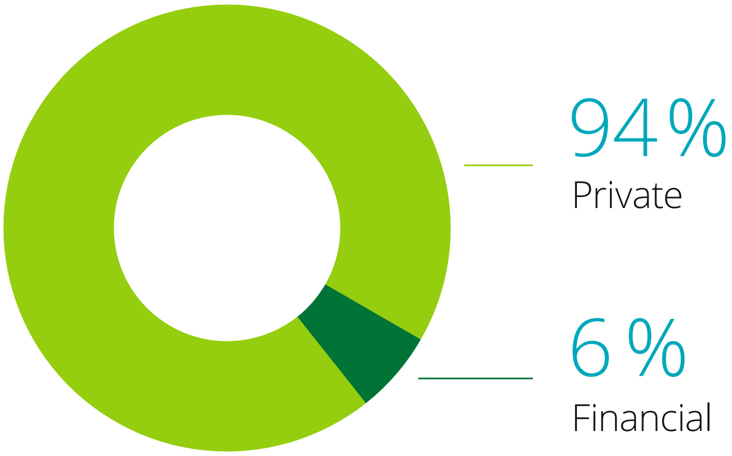
Certain types of IT assets pose an additional risk to the resiliency of your organisation – for example Active Directory servers that contain your user hierarchy and access rights or your backup systems. We recommend security hardening these systems against a cyberattack, for example, by implementing malware protection software or white-listing of the applications that are allowed to run on these systems. This will help contain the damage from a cyberattack and enable faster recovery.

About the research & contacts

Employee split



Sector split



The 2019 Cyber Risk Landscape Survey comprises data from 118 major Danish private and financial sector companies. It focuses in particular on parameters such as maturity, incident response readiness and executive awareness on cybersecurity.

The study is based on a quantitative questionnaire survey conducted by way of CATI (computer-assisted telephone interviews). In total, 118 leaders responsible for cybersecurity participated in the survey.

The fieldwork was performed from October to November 2018 by Epinion (a research and insights management solutions company) based on a set of questions provided by Deloitte Denmark.

For further information about this research, please contact:

Serdar Cabuk, Ph.D.
Partner, Nordic Cyber Leader
+45 30 93 50 70
scabuk@deloitte.dk

Endnotes

1. Forsvarets Efterretningstjeneste. Efterretningsmæssig Risikovurdering 2018. 2018. URL: https://fe-ddis.dk/Produkter/Risikovurderinger/Pages/Efterretningsmaessigrisikovurdering2018.aspx

2. World Economic Forum. Global Risks of Highest Concern for Doing Business. 2017. URL: http://reports.weforum.org/global-risks-2017/global-risks-of-highest-concern-for-doing-business-2017/#

3. BT. Bahne.dk udsat for nyt hackerangreb: 'Det er en katastrofe'. 2019. URL: https://www.bt.dk/forbrug/bahne.dk-udsat-for-nyt-hackerangreb-det-er-en-katastrofe

4. ComputerWeekly.com. IT security hindering productivity and innovation, survey shows. 2017. URL: https://www.computerweekly.com/news/450428565/IT-security-hindering-productivity-and-innovation-survey-shows

5. Deloitte. Global Defense Outlook 2016. 2016. URL: https://www2.deloitte.com/global/en/pages/public-sector/articles/gx-global-defense-outlook.html

6. Forbes. The Cybersecurity Talent Gap Is An Industry Crisis. 2018. URL: https://www.forbes.com/sites/forbestechcouncil/2018/08/09/the-cybersecurity-talent-gap-is-an-industry-crisis/#5e0dab33a6b3

7. TV2. Det sejler for mange steder, lyder vurdering efter afslørende hacker-undersøgelse. 2018. URL: http://nyheder.tv2.dk/samfund/2018-05-14-det-sejler-for-mange-steder-lyder-vurdering-efter-afsloerende-hacker

8. Verizon. 2016 Data Breach Investigations Report. 2016. URL: https://enterprise.verizon.com/resources/reports/DBIR_2016_Report.pdf

Deloitte.

This publication contains general information only, and none of Deloitte Touche Tohmatsu Limited, its member firms, or their related entities (collectively, the "Deloitte Network") is, by means of this publication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser. No entity in the Deloitte Network shall be responsible for any loss whatsoever sustained by any person who relies on this publication.