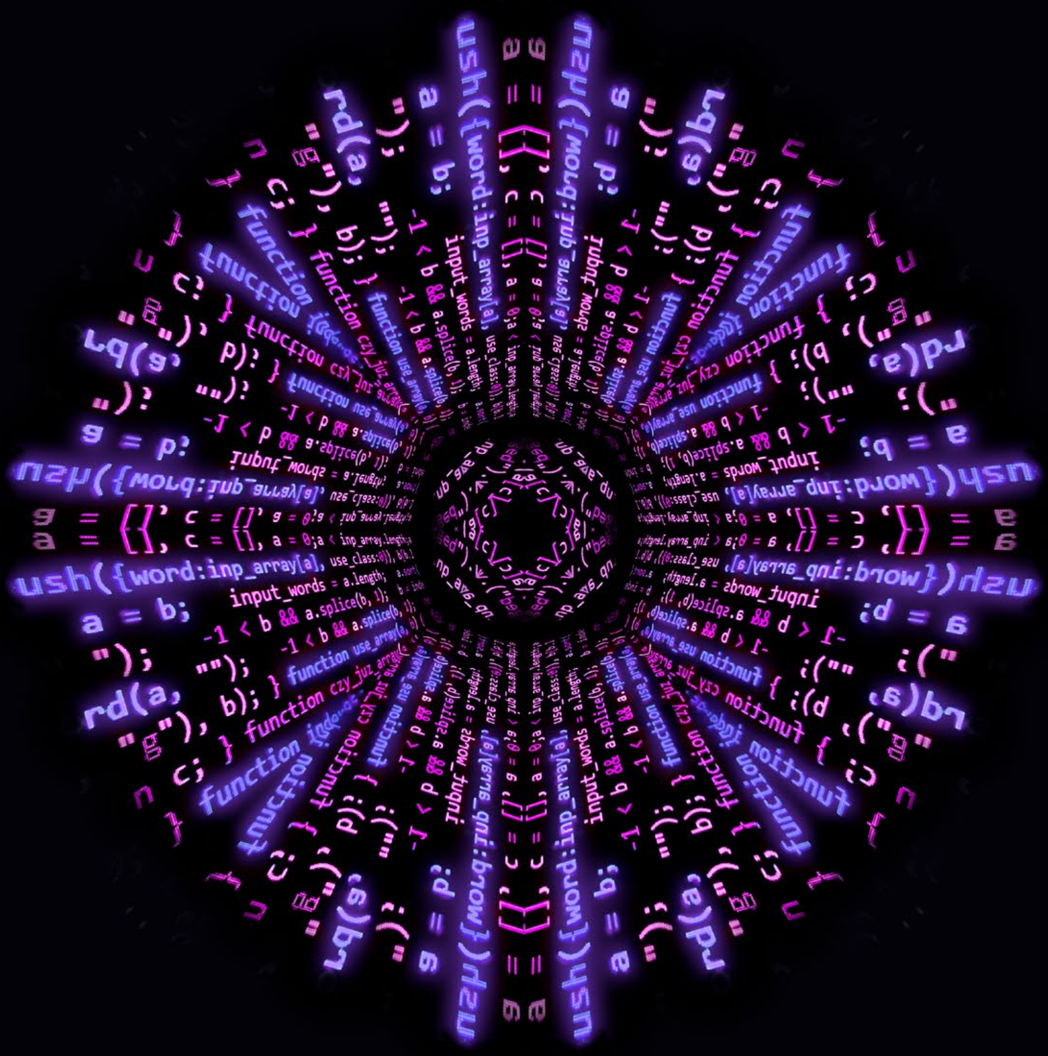
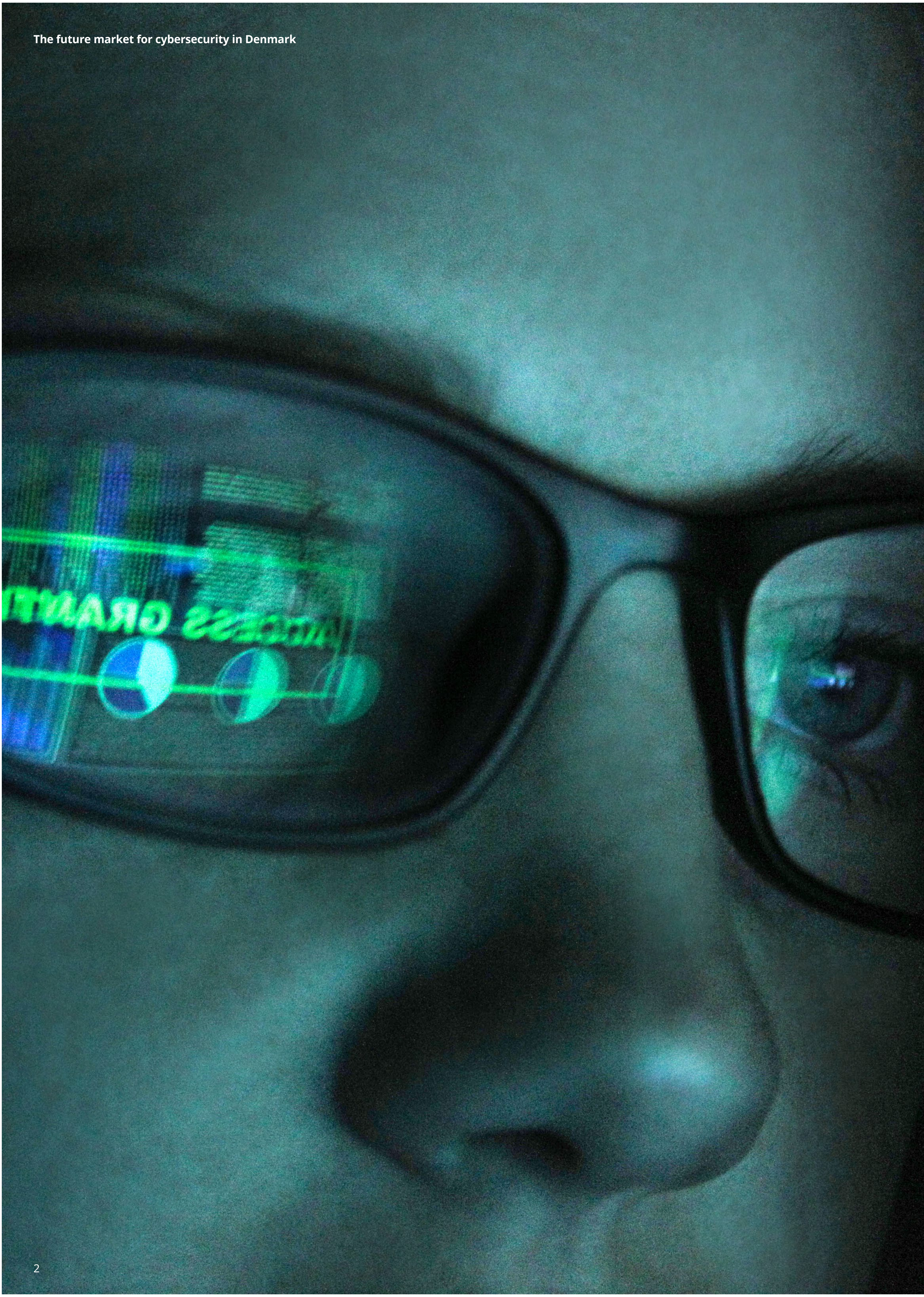
Deloitte.

Innovation Fund Denmark

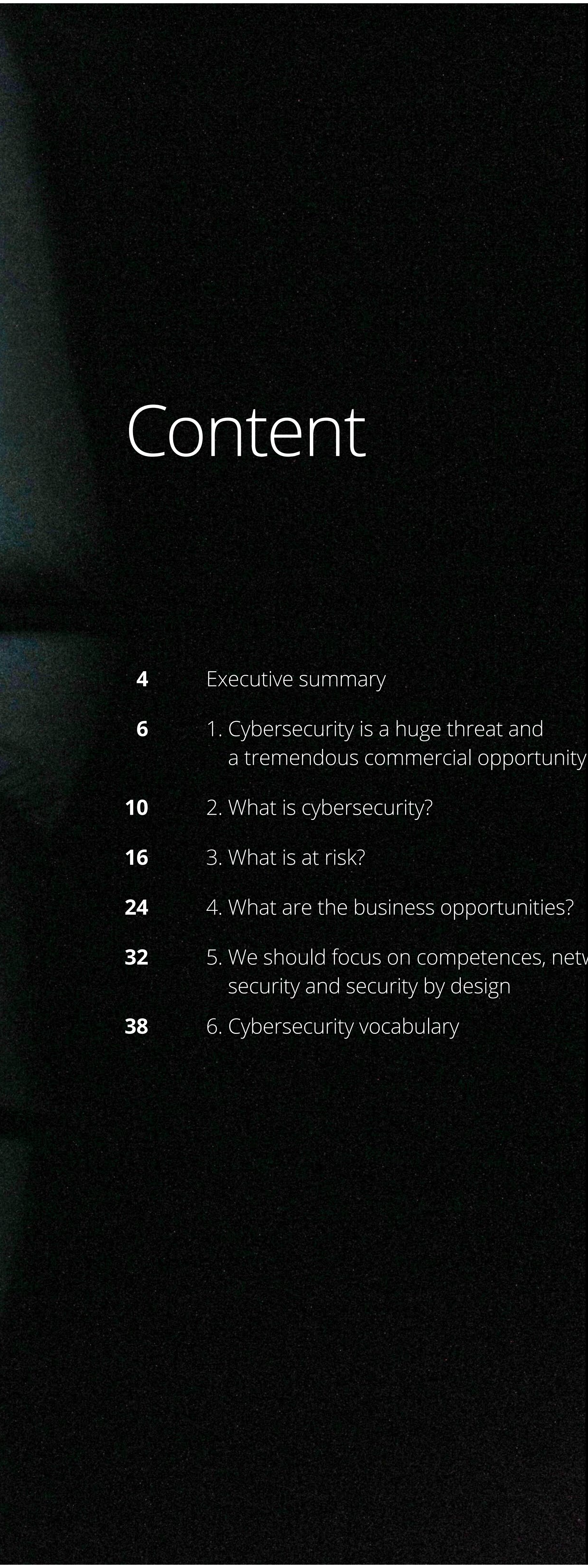
ALEXANDRA INSTITUTE



The future market for cybersecurity in Denmark



ACCESS GRANT



Content

Contributors to the final report

Innovation Fund Denmark
Peter Høngaard Andersen
Tore Duvold
Michael Adsetts Edberg Hansen

Alexandra Institute
Ole Lehrmann Madsen
Gert Læssøe Mikkelsen
Laura Lynggaard Nielsen

Monitor Deloitte
Michael Hjortlund
Carina Jensen (editor)

Deloitte
Lars Syberg
Erik Lind Olsen (editor)

Executive summary

The cyber-threat is significant and growing fast. This poses a challenge for us all, and everyone needs to consider it and act on it. The good news is that Denmark can take a leading position in the exploding market of cybersecurity – if we act fast.

Cybersecurity is best described as a game with an offender and a victim. Every time we suffer the consequences of an attack, we learn to protect ourselves better – and, every time, the offenders find new routes or methods. In other words, we can never be 100 percent secure, and that is not the goal. Instead, cybersecurity is like conventional crime prevention: we should focus on making it difficult and risky to commit cybercrime and minimise the impact of an attack.

Authorities, infrastructure providers, companies, organisations and individuals all face separate challenges related to cyber-risks, but they are also highly interconnected. In today's digital society, we are all connected and data is distributed across platforms, systems and servers. This means that we do not only need to consider the direct risks we face, but also the indirect risks from interacting with others. Digitalisation and cybersecurity are two sides of the same coin.

Currently, Denmark is far from taking a leading position on cybersecurity. On the contrary, several reports document that we are lagging behind. However, we have the preconditions to not only catch up, but also to become a frontrunner in developing security solutions for a global market, a market that will see high growth and probably mature rapidly in the coming years. However, we need to act fast to reap the potential benefits in time.

Two trends will drive growth in the market for cybersecurity by creating a demand for new types of cybersecurity activities: open networks and digitalisation of the objects around us. Both trends put the actions of individuals and societies in focus – not just the protection of the outer wall of organisations and companies.

To capture a large share of the potential market, companies and the society need to act. As a positive side effect, the actions will increase our cybersecurity at all levels of society.

We have identified three main levers based on input from a wide range of experts, scientists, entrepreneurs and lead users:

1. **Cybersecurity competences**
   To raise competences at all levels, we must 1) include cybersecurity in common education and regulate cybersecurity training requirements for companies and professions; 2) continue campaigning for a better general understanding; 3) invest in public research relevant to cybersecurity and 4) increase collaboration across sectors.

2. **Secure traffic and networks**
   Today, the focus is mainly on securing the perimeter of organisations. In an increasingly open internet, security solutions must emphasise safe traffic and individual usability. To this end, we must invest in focused research, set national standards and stimulate innovative cross-disciplinary solutions.

3. **Security by design**
   Many products lack cybersecurity measures by default, which increases the vulnerability to cyberattacks. We should develop a new production paradigm based on security by design through national standards and certifications, continuous development of best practices in different industries and promotion of usability in cybersecurity solutions.

1. Cybersecurity is a huge threat and a tremendous commercial opportunity

Cybersecurity is big business. It used to be a concern for the IT department and paranoid types in tin-foil hats. Now, every responsible company and organisation look at recent breaches and ask: could this happen to me?

Yes, it can – and it most likely will. In the spring of 2017, the WannaCry attack infected more than 200,000 victims in over 150 countries. Among them was the British National Health Service (NHS), who was forced to postpone surgeries. Later the same year, Danish shipping giant, Maersk, was brought to its knees by the global NotPetya attack, which affected business globally and cost more than 200 million dollars[1].

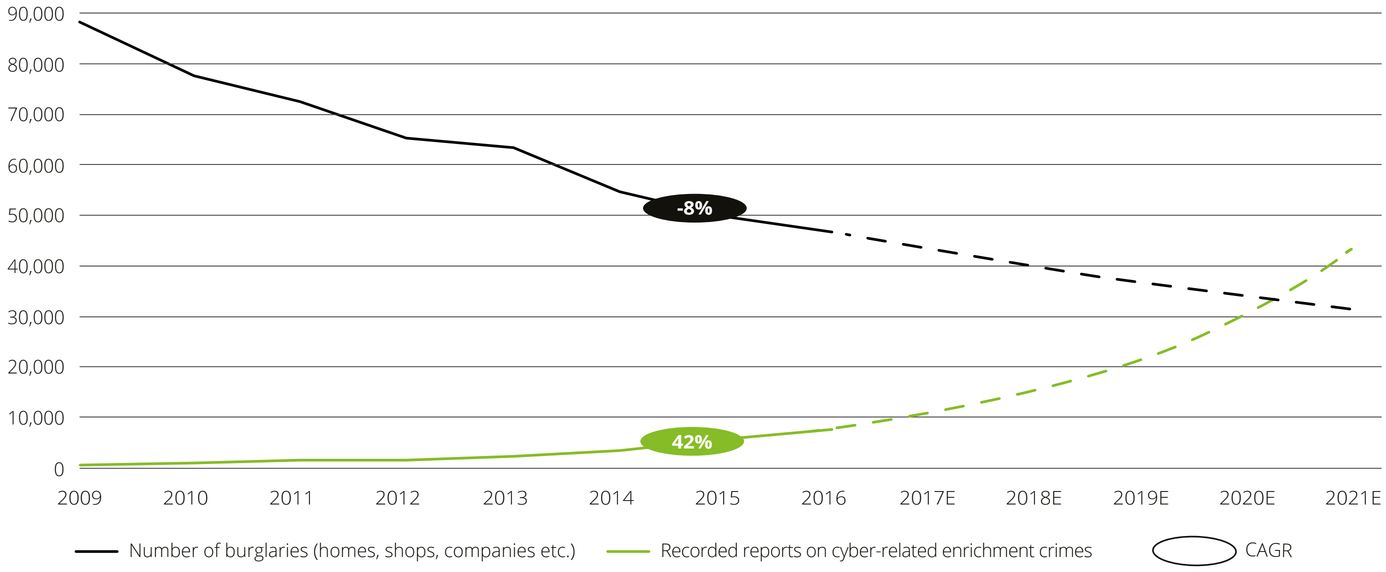
This is just the beginning. In the coming years, cybersecurity will spread from corporate agendas and become a household issue. As more and more products and processes become digital and cloud solutions spread, we all have to consider cybersecurity in the same way we consider the safety of our home.

We must protect our lives from cybercrime just as we try to keep burglars out of our homes. With the current trends, cybercrimes will be more common than burglaries in less than three years.

We are in the same position as the rest of the world. The great risk from cyberthreats therefore also represents an opportunity for the countries and companies. A global market is bound to materialise and the ones who develop the best cybersecurity solutions win.

> ”Earnings from cybercrime are higher than drugs now – and everyone can order an attack.”

Figure 1. Reported burglaries and cybercrimes



Sources: Danish Police, Danmarks Statistik

[1] www.bbc.com, www.forbes.com

1.1. We aim to make Denmark and Danish companies winners of the race

This report sets out to put cybersecurity on the strategic agenda for companies and authorities by focusing on both threats and commercial opportunities. The ambition is to turn a massive threat into an attractive opportunity by concentrating on Denmark's potential in developing cybersecurity competences and solutions as well as on the opportunity for Danish companies to use cybersecurity as a differentiator.

We look into three topics:

- **What is cybersecurity?**
  We establish a terminology for the discussion of cybersecurity to make the subject accessible to all potential stakeholders. Our approach is to digest the vast literature about the subject and present a simple overview.

- **What is at risk?**
  We describe the threats to authorities, companies, individuals and society as a whole. We build an understanding of current and emerging risks from expert interviews and workshops with companies and organisations interested in cybersecurity.

- **What are the business opportunities?**
  We show the potential for services and offerings related to cybersecurity based on projections of threats and trends. Our analysis combines research of market data and expert inputs about the development.

Based on these three topics, we present our recommendations for national focus areas in chapter 5.

The results are disclosed openly to stimulate market awareness and business development for Danish operators in the field as well as to create greater awareness on the subject among companies, authorities and the broader society.

We refer directly to our written sources of information. Interview and workshop input is anonymised but illustrated in the highlighted quotes. The participants are described in more detail on page 42.

1.2. We focus on the protection of information and systems

The focus of this report is the protection of digital information and systems. We are focusing on cybercrime in instances where the aim is to get access to any kind of digital information or system against the will or knowledge of the owner.

With this focus, we explicitly exclude two topics:

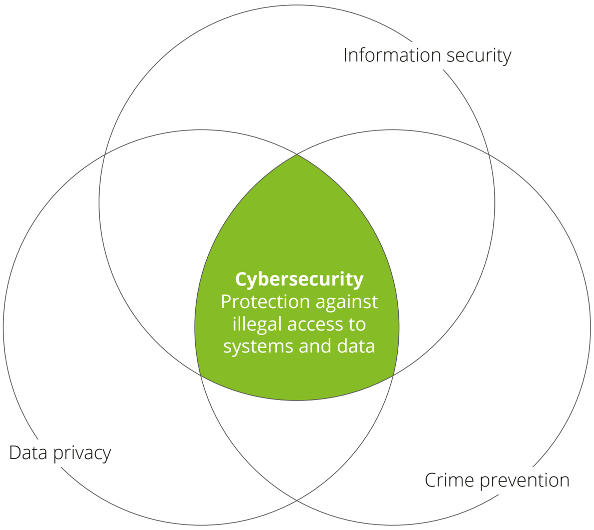
1. Physical access control: Physical access to information or systems to cause harm – for example through steeling a USB key to gain access to the content or breaking into a building to shut down a system – is not among the security threats addressed. This means that physical access control is excluded from this report, but manipulation of software in a physical device to get access to information or systems is included.

2. Criminal content: Distribution of illegal or illegitimate content through digital channels - for example illegal digital pictures or deliberate spread of disinformation, unless they are part of a scheme to get illegal access to systems or information – is also excluded.

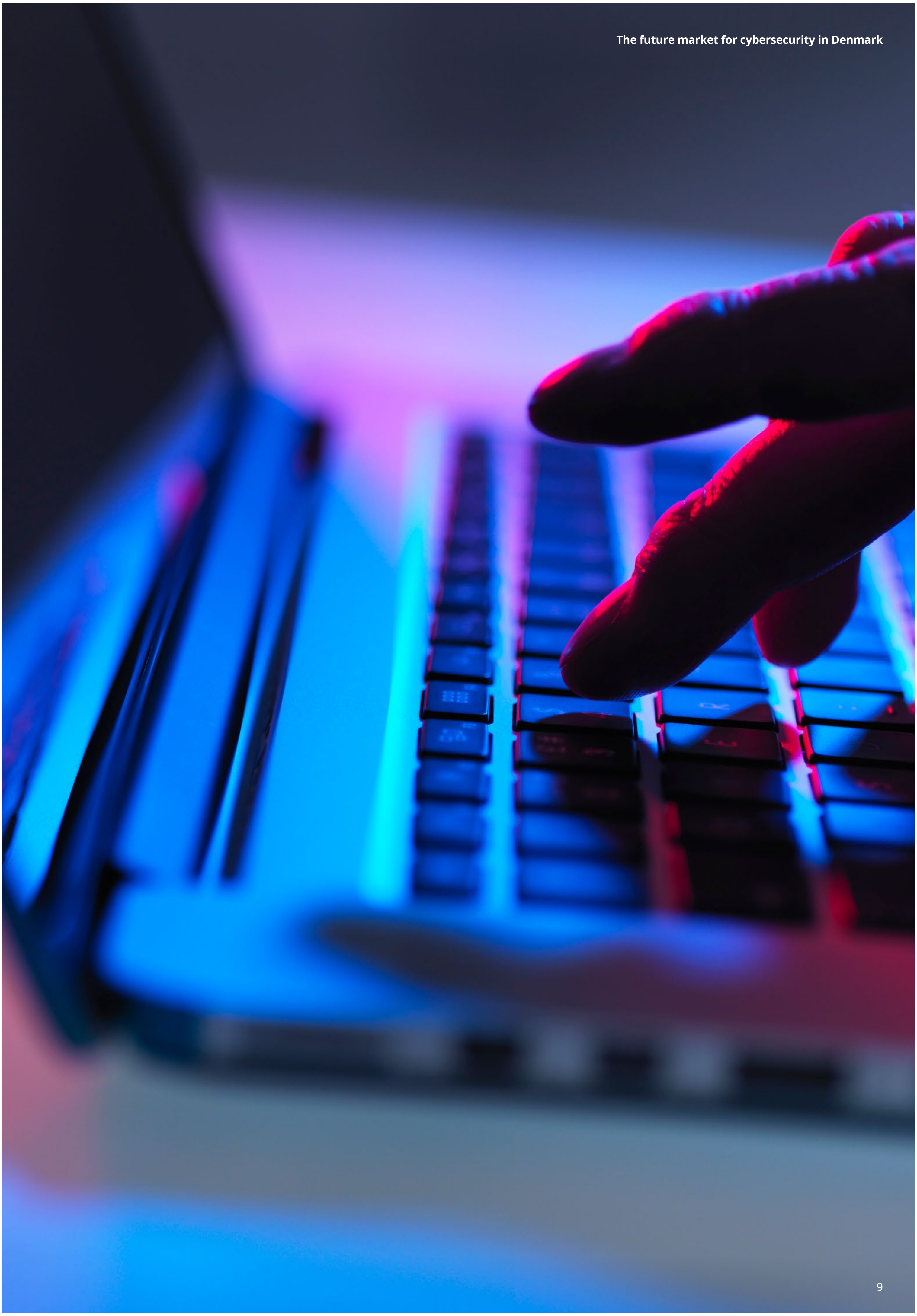
Data privacy has gained a lot of attention recently due to tougher regulation[2], and data privacy seems inevitable when discussing cybersecurity. However, we will not include a full description of the data privacy subject. The focus of the report is the threats and protection against criminal actions, not data rights.

However, the topic will be discussed from a solution perspective as data privacy has a close link to cybersecurity from a user perspective. The user often perceives cybersecurity and data privacy as one issue. Furthermore, the GDPR serves as an example of the positive effect that tighter regulation can have on investments in cybersecurity.

Figure 2. Focus of the report



[2] EU GDPR (General Data Protection Regulation) taking effect from May 2018



2. What is cybersecurity?

Cyber-risks pose a great threat for authorities, companies and citizens. In addition, cybersecurity is becoming a widely discussed topic and is continuously gaining attention from both the public and the media. We have seen this increased attention in the newly updated Danish Defence Policy, which allocates 1.4 billion Danish kroner to improve the Danish cyber-defence. We also see that the media increasingly covers cyberattacks and breaches. Consequently, it is highly evident to everyone that cybersecurity is crucial.

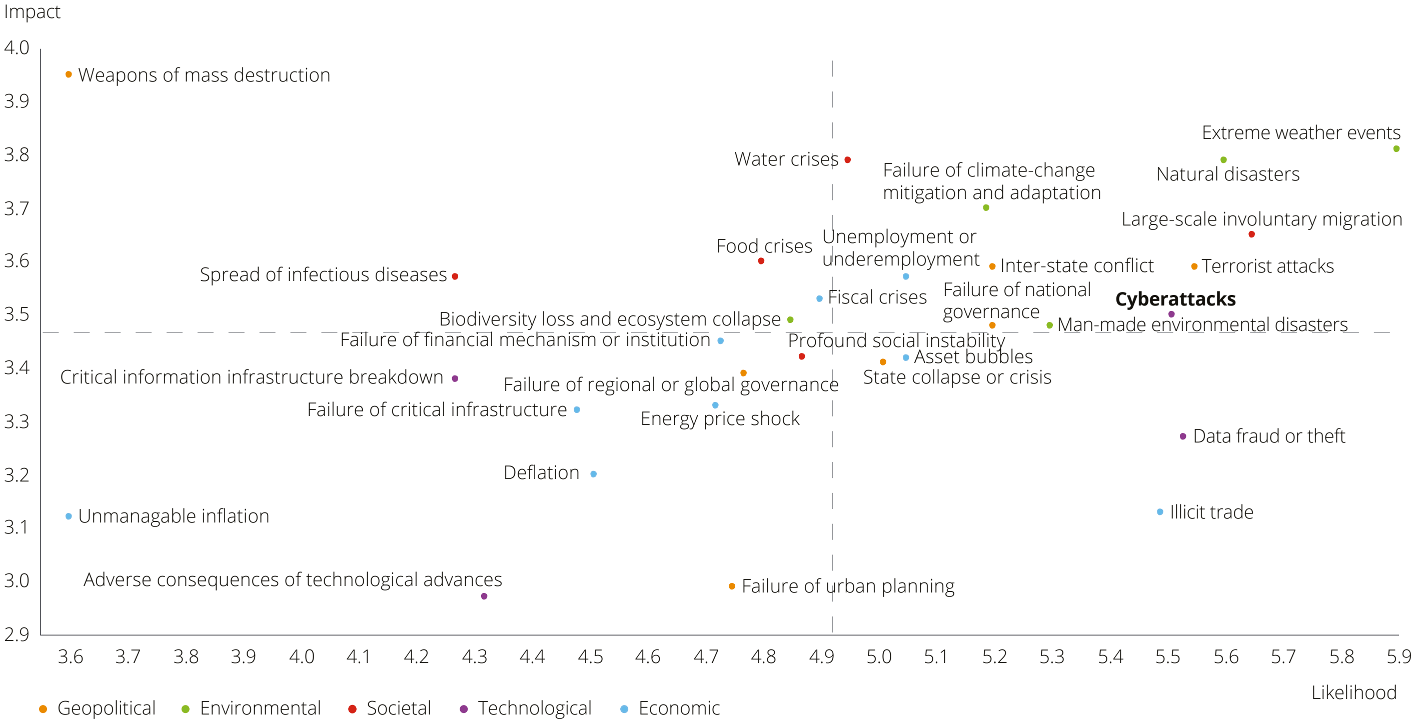
As attention increases, the link between cybersecurity and digitalisation becomes stronger. We cannot maintain growth based on new digital developments if we do not address the security of the solutions.

Today, cybercriminals are not just individual hackers sitting in their basements acting on their own. They have become organised criminals, whose business model is to generate revenue from cyberattacks. For the criminals, their actions carry low risks, as they are difficult to identify. Furthermore, there is a great incentive to carry out cybercrime, for example in the form of ransom money. Many criminals also offer their skills as a service to others. The result is that cybercrime is becoming available to the public: everyone can buy an attack.

Cyber-risks are indeed an issue to address. The Danish Center for Cybersecurity evaluates the cyber-threat against Denmark each year. In 2017, they estimated the threat from cyberespionage and cybercrime to be very high . The threat is not just present in Denmark though, but also on a global scale. Globally, cyber-risks are one of the most prevalent risks, and the World Economic Forum estimates it to be the risk that is sixth most likely to materialise.

Figure 3 maps the global risks as analysed by the World Economic Forum. The x-axis measures the likelihood of the risk, and the y-axis measures the impact of the risk. The dotted lines show the average impact and likelihood of all the risks included, which places cyberattacks above average on both parameters. The risk of cyberattacks is on level with terrorist attacks in terms of likelihood and impact. Equally high on the likelihood scale but with a lower impact, we find data fraud and theft.

Figure 3. Global risks mapped based on impact and likelihood



Sources: World Economic Forum 'Global Risks Report 2017'

Note: Each measure has been qualitatively evaluated on a relative scale from 1-7.
The area shown is the part of the scale where the most likely and impactful risks were placed.

[3] Center for Cybersikkerhed, "Trusselsvurdering Februar 2017".

Despite the high risk, there is still an overall lack of awareness about cyber-risks and cybersecurity in Denmark. We see this in companies, where responding to cyber-risks are on a seventh place when you ask C-level executives what they discuss over the course of a year. Only 24 percent of C-level executives expect cyber-risks to have an increasing impact on their organisation over the next five years[4].

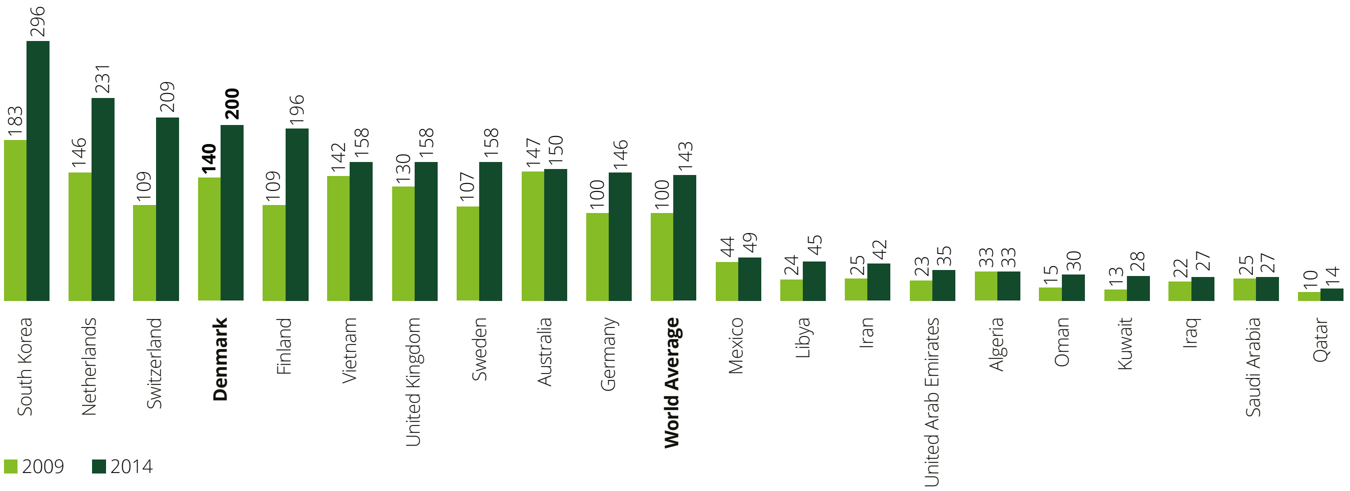
Denmark ranks as the most digitalised country in Europe[5], which entails a high degree of vulnerability. Denmark's high level of digitalisation increases our vulnerability to cyberattacks and places us among the most vulnerable countries in the world – and the vulnerability is increasing fast, as can be seen in Figure 4.

Based on our expert interviews, we find that the reason for the imbalance between digitalisation and cybersecurity is threefold:

- First, cybersecurity is generally difficult to get right. Many companies do not recognise the extent of the challenge, and when they do, it is difficult to define a business case upfront and evaluate the benefits from implementing cybersecurity measures. Consequently, organisations and companies all over the world tend to underinvest in cybersecurity measures.
- Second, Denmark has a high level of digitalisation – especially in the public sector - and we quickly adopt new technologies. The fast adoption is a challenge, because most of the new developments emphasise speed over security. Furthermore, as the technical solutions are becoming more complex, it gets more complicated to get a full overview of the vulnerabilities.
- Finally, the Danish culture is built on trust. We find it uncomfortable to challenge partners about security and risk assessments, and we expect strangers to have good intentions. This bias permeates fast adoption of new digital solutions and underinvestment in security - and makes us one of the most vulnerable countries in the world.

We must emphasise that this curse can also become a blessing. Our fast adoption rate and our preference for trust-based cooperation are also part of the reason why we have high hopes for Denmark. We see Denmark as an obvious laboratory for the development and testing of new solutions.

Figure 4. Cyber-Vulnerability Index



Sources: Deloitte, "Global Defense Outlook 2016"

Note: The numbers are indexed based on the world average in 2009, which served as index 100. The status for each country is then calculated based on the World Development Indicators of the World Bank on rate of mobile cell subscribers, number of secure internet servers, fixed broadband subscribers and rate of internet use. Overall, the index relies on internet-based interactions in each country and not security measures.

[4] Deloitte Insights "The Fourth Industrial Revolution is here – are you ready?", 2018.
[5] European Commission, DESI profile 2017, Denmark.

2.1. Cybersecurity can be understood as a game with an offender and a victim

Cybersecurity is hard to grasp for most companies, organisations and individuals. A reason for this is that cybersecurity is somewhat diffuse, and we are lacking a common framework for discussing cybersecurity. This section intends to provide an overview of the main concepts and link these to the primary types of cyberattacks. Cybersecurity can be seen as consisting of seven elements, as shown in Figure 5, and is best understood as a game with an offender and a victim.

We start our description from the perspective of the offender, as the activities of the victims are a reaction to experienced or anticipated attacks. In Figure 6, there is an overview of each element, and each element is described in detail in the cybersecurity vocabulary in the appendix.

1. The offender can have different **motives** for their actions. The most common motive is economic gain, but activism, vandalism, espionage or even terrorism are other possible motives behind cyberattacks.

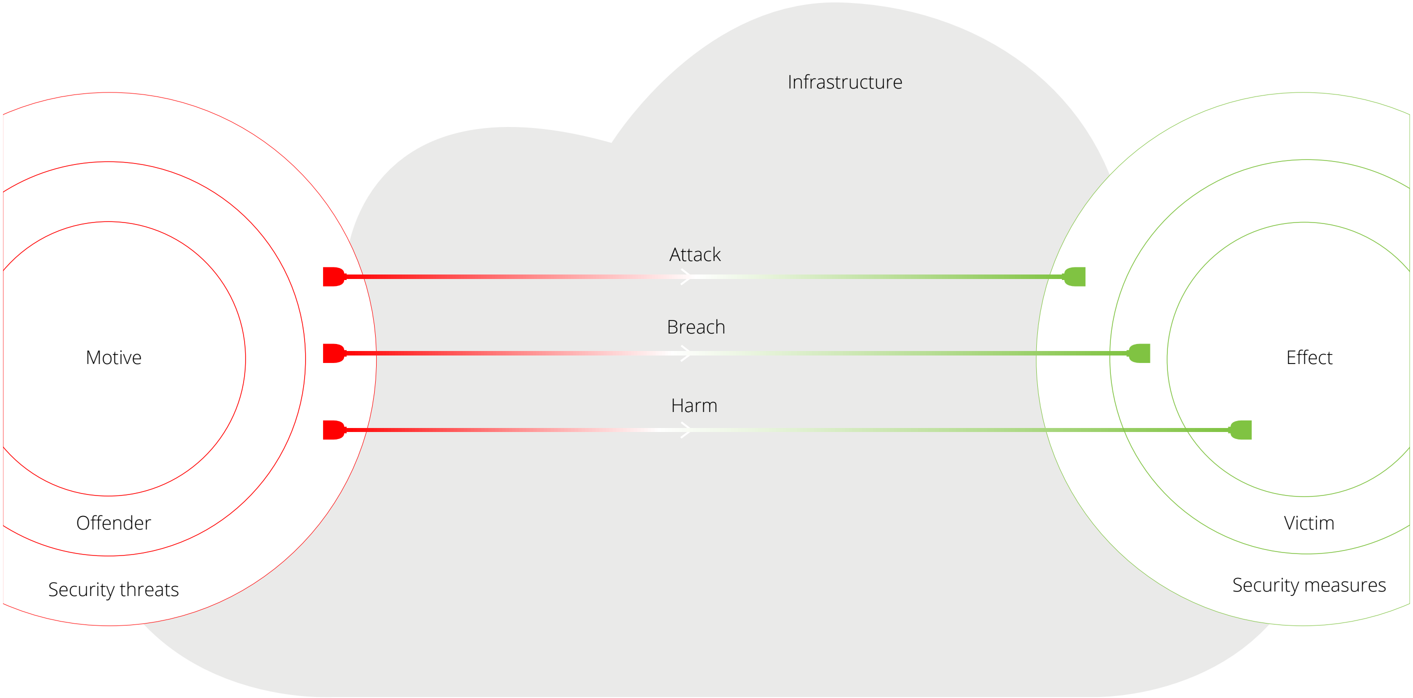
2. The motive depends on the **offender**, and again there are a number of possibilities. The offender can be an individual (even an employee), a competitor, terrorists, organised criminals or foreign states. In some situations, there can be multiple offenders, for example if a company hires a group of organised criminals to carry out a cyberattack on a competitor.

3. Many different **security threats** are available to the offenders. The offender can manipulate their way to gain access to data or systems. They can install malicious software on the victims' computers or systems, or they can hack their way directly into systems to get data or control. The offender can also attack their victims by overloading their servers and thereby slow down their systems or completely shut them down. The offender can also hire professional criminals to carry out the work; this is known as crime-as-a-service.

4. Cyberattacks take place in a digital **infrastructure**. When we describe the infrastructure, we distinguish between channels and vectors. The channels are the different digital areas where offenders and victims are present and meet. The vectors are the means for carrying out the attack using weaknesses in networks, devices, applications or human behaviour to gain access.

5. The potential victims have a number of **security measures** at their disposal to prevent or handle attacks. Some focus on the network to detect potential threats or secure internet traffic between organisations or households. Other measures relate to the devices and the applications run on them. These measures typically prevent or handle the entry of unwanted code or access

Figure 5. The basic terminology of cybersecurity



to the data on the device or on a shared server. The last category deals with human behaviour and with how breaches caused by humans can be prevented and dealt with if they occur.

6. Potential **victims** fall in four different categories. They have different risk profiles that should be reflected in the cybersecurity approach:

- Authorities have a special position as legal regulators and protectors of the society.

- Network and information systems (NIS) are companies or organisations that provide physical and digital infrastructures for others , and they are therefore crucial to society[6].

- Other companies and organisations are also potential victims of cybercrime.

- Individuals can be the target of a cyberattack, either in their own right or as part of the other categories.

7. To understand the **effect** of a cybercrime, we must distinguish between attacks, breaches and harm. Without knowing, every individual and organisation are subject to random attacks every day. Many attacks go unnoticed because we have the right measures in place, for example a firewall that stops the attack. Some attacks are technically successful and lead to a breach, for example when someone gains illegal access to systems or data. Many breaches go unnoticed for long periods and give the intruder the opportunity to spy on the victim or wait for the best time to cause harm, for example by stealing data or taking over a transaction. On average, it takes organisations more than 190 days to detect a cybercrime and more than 65 days to contain the breach and resolve the situation[7].

In Figure 6 there is an overview of all the elements mentioned above. This overview can serve as a basis for understanding cybersecurity as we are discussing it.

> “Crime-as-a-service, where ordinary people can buy an attack, is increasing. We have for example seen students order attacks on their schools to get out of an exam.”

Figure 6. Cybersecurity elements

Motive	Offender	Security threats	Infrastructure	Security measures	Victim	Effect
Intention • Economy gain • Activism • Espionage • Vandalism • Terror • Misinformation/ fake news	Offender • Individuals • Internal employees • Organized criminals • Companies • States and governments • Terror groups	Method of attack • Manipulation - Phishing - Smishing - Social engineering - BEC - Credential harvesting • Malicious installations - Malware - Ransomware - Adware - Spyware • Hacking - Targeted intrusion - Opportunistic targeting -Exploits • Server overload - DDos - Botnet	Channels • Network - Internet - Critical infrastructure - Wireless networks • Devices - Hardware - Mobile devices - Servers - Autonomous devices - Robot - Internet of Things - Supply chain • Applications - Software • Behavior - Employees Vector • Emails Remote Command Execution Watering hole Physical devices	• Network - Traffic monitoring - Encryption • Devices - Access control - Security updates - Safe sensors/supply chain • Applications - Firewalls - Antivirus - Patching - Backup - Monitoring - Computer logging - Spam/mail filters - Blocking - Analyses and tests - Documentation • Behavior - Training - Analyses and tests - Documentation - ISO standards - Procedures - Strategy	• Authorities • Network and Information Systems • Companies and organizations • Individuals	• Attack • Breach • Harm

[6] NIS companies are public and private companies that provide electricity, oil, gas, air transport, rail transport, water transport, road transport, banking, financial infrastructure, healthcare, drinking water supply and digital infrastructure, for example online marketplaces, online search engines and cloud computing services.

[7] Ponemon Institute ”2017 Cost of Data Breach Study, Global Overview”.

3. What is at risk?

There are many risks related to having insufficient cybersecurity and cyberrisks are prevalent across society. From the terminology, it becomes evident that overall, there are four types of victims. They all face specific types of risk, but they are highly interrelated. Therefore, it is necessary to understand the risks they face separately, but also to understand how they are connected. In all these categories, there are technology, people and organisational factors that affect the perception of cyberrisks, how they are mitigated and how they can affect the actors. Another common denominator is that the risks for all actors are highly related to financial risks as it will often have financial consequences to recover from a cyberbreach.

The risks from cyberattacks are best understood if you see them in relation to the benefits of digitalisation. The victims all face great cyberrisks that they need to protect themselves from. At the same time, they need to balance this with a desire to be open to reap the benefits of digitalisation. Figure 7 visualises this dilemma by showing what is ultimately at risk for each actor.

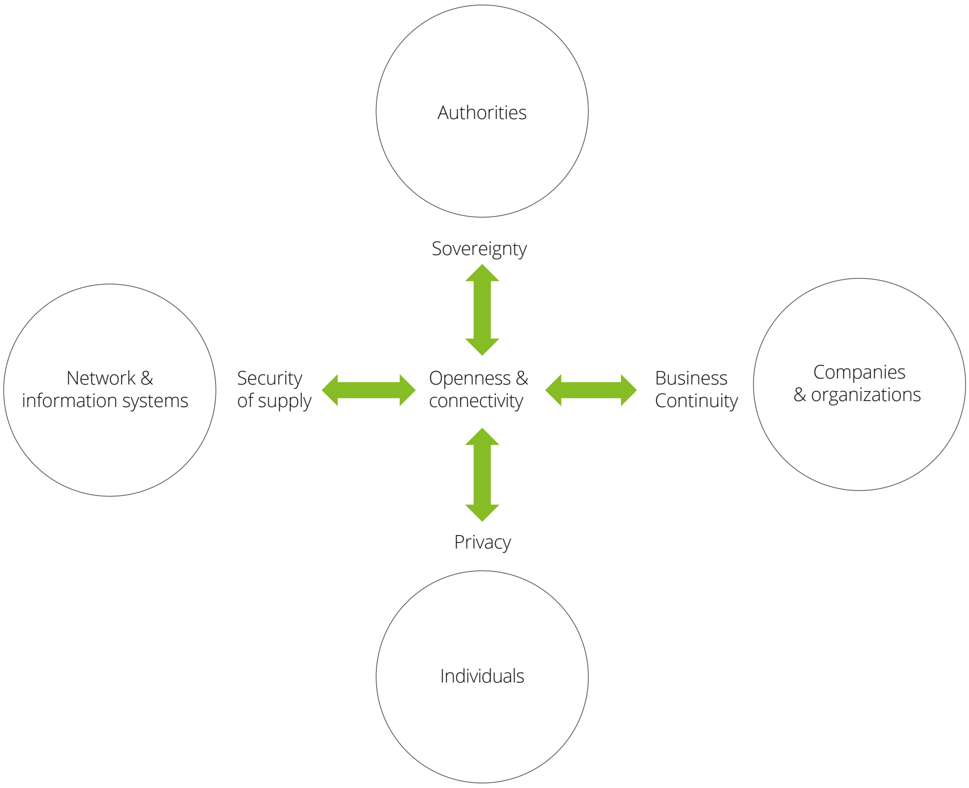
For all actors, cybersecurity is a question of balance between being part of the digital development while protecting themselves. Up until now, the desire to be open and connected has trumped most other concerns. The consequence is thus that digitalisation has created a high level of risk.

In the following, we will describe each of the victim categories. It is important to note that even though we have separated the individuals, there are of course people who belong in all of the other groups.

Individuals can stimulate the security as employees and as consumers:

- Individuals as employees are a key element in cybersecurity for all the actors. Individual awareness and competences are important because most methods for intrusion rely on human errors
- Individuals as consumers stimulate demand for cybersecurity in the products or services companies provide. The more concerned the individuals are, the bigger the demand for secure products

Figure 7. Risk and benefits for different groups



3.1. Authorities carry a special obligation in relation to cybersecurity

The authorities are a vital part of the Danish society, and they have a great responsibility for the functioning of our fundamental institutions. They are in daily contact with citizens and organisations and therefore need to be open and accessible. At the same time, they need to balance this with the risk of losing control and ultimately sovereignty, for example if foreign states, terror groups or companies get access to or tamper with vital data or systems. This can have great impact on the authorities themselves but also the citizens, organisations and society as a whole.

> ”We must protect the outer borders to protect our state and nation. There is a lot of foreign activity and it is therefore fundamental for our society to have data protection.”

In general, public data systems in Denmark are highly centralised, which makes it easier for citizens to use them. At the same time, it increases the authorities' overview of and accessibility to information about citizens. We have one point of access to public systems and bank systems (NemID) and one identification number used across all parts of society (CPR). This increases convenience but also vulnerability. A cyberbreach in one place can quickly spread to other parts of the system. These systems serve as single points of failure, which therefore impose great risks.

A cyberbreach can have a critical impact. Authorities store massive amounts of data about citizens and organisations. This covers for instance medical history, salary and tax information about citizens, and patent information or revenue data about companies. All this information is very sensitive and a data leak can therefore have great consequences. For individuals, it can have personal consequences, and for companies it can affect their competitiveness and stability.

> ”80 percent of the incidents that the data protection agency handles are public incidents.”

To increase the level of cybersecurity, authorities can initiate protective measures on a national level, and at the same time do collaborative efforts with other national authorities, for example on an EU level. The authorities also have the opportunity to increase cybersecurity on a societal level by raising general awareness.

Even though, national authorities store more data and have a crucial role in society, they face the same cybersecurity challenges as other organisations. If they take a strategic approach to cybersecurity and implement relevant measures, they can take a position as role models and lead the way for the rest of society. This can for example be in regards to GDPR[8] being as least as important for authorities as for companies.

3.2. NIS companies are responsible for security of supply

NIS are companies delivering basic infrastructure to the society. They are responsible for the security of supply and play a key role in ensuring that society is running at full speed. They accomplish this by being open to collaborate and interact with other actors while sharing data and information.

New NIS directive

In August 2016, the European Commission publicised a new directive on cybersecurity for Network and Information Systems (NIS Directive). The intention of the directive is to boost the overall level of cybersecurity in the EU. The countries have 21 months to transpose the Directive into their national laws and six additional months to inform operators of these essential services[9]. This means that the new directive will soon come into effect. It requires all NIS companies to take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of the systems they operate. In addition, NIS companies are required to implement measures that can both prevent and minimise any cybersecurity incident. Moreover, NIS companies will be obliged to notify authorities of any incidents having significant impact on the continuity of the services they provide. There will be penalties to the NIS companies if they do not live up to the requirements, but these are yet to be determined[10].

[8] EU General Data Protection Regulation
[9] https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive
[10] EU directive 2016/1148

Due to NIS companies' key role in society, the cyberrisk facing them will not only affect the companies and organisations themselves, but all levels of society. A disruption in their service can thus both affect and harm other actors. As such, cybersecurity in these companies are critical and it is relevant to openly question if existing efforts are sufficient. Other organisations are also asking whether these companies, for example phone companies, should take greater responsibility for the cybersecurity of the products and services they provide, for example through more monitoring of abnormal patterns in the traffic on their networks.

Security of supply is not only threatened by cyberthreats but is part of a larger risk picture. Cybersecurity measures are therefore heavily connected to other security measures in assuring security of supply, for example physical protection. For cybersecurity measures, NIS companies have a big challenge in scaling their cybersecurity, as they have major networks with many ramifications. This requires cybersecurity in all ends – many of which are at the consumer's end where the NIS company does not have full control.

For NIS companies there is also a need for contingency planning to enable a rapid response in case of a security breach. As the continuous running of these companies is crucial for society, it is important to be able to quickly detect and solve problems in case of an outage.

Sandworm hits power plants
In December 2015, a large part of Ukraine lost electricity for six hours. Three power plants powered the area and these were all taken down simultaneously by a malware called "KillDisk". KillDisk had entered the systems through a phishing mail that contained a malicious Word attachment. Once the attachment was open, it ran a silent script in the background. The offenders appeared to be a group known as "Sandworm" that is believed to be Russian. They had previously attacked Polish energy firms and Ukrainian government agencies. The malware was also found on US grids, but was removed before it was set in motion. In December 2016, Ukrainian power plants were hit again. This time, they were only down for one hour but experts found the code behind it to be much more sophisticated. Again, Sandworm was believed to be the offender[11].

3.3. Other companies and organisations risk leaking critical information about themselves and their stakeholders

Most other companies and organisations interact with customers and other stakeholders and want to be open to learn from customer data. At the same time, they need to secure the data about these stakeholders as well as protect their own data and the systems critical for their business and competitiveness. This concerns what is going on inside the organisations but also the safety of the products they sell. As physical products become digital they entail a growing potential to be exploited. The purpose is of course to protect the data and systems of the company, but they also need to ensure credibility and trust from consumers in order to reap the full benefits of digitalisation.

> "It is important to see your products at a client site as part of your infrastructure, and it is necessary to extend your cybersecurity to include this as well."

Behind many organisations, we find a number of suppliers and subcontractors who pose a threat to the organisation. Not only from the data flowing between them but also through the products, components and services they procure. This expands the focus of cybersecurity to include the organisation's entire supply chain.

> "If you cannot get direct access to a company, you will go through their suppliers."

[11] https://www.wired.com/story/russian-hackers-attack-ukraine/

However, organisations struggle to economically justify investments in cybersecurity, as many do not see the business case. Currently, their customers are not demanding cybersecurity and the organisations do therefore not see the economic advantages in offering this. At the same time, they have trouble identifying what is ultimately at stake if they do not invest.

Many organisations are therefore asking for cybersecurity certifications that can both serve as guidelines for companies on what to achieve and show consumers which organisations are secure. On the one hand, certification can create more awareness about cybersecurity and give organisations a way to differentiate. On the other hand, certifications can build a false sense of security as it is impossible to build solutions that are 100 percent safe. Parallels can be drawn from the car industry where safety measures are tested and rated even though the driver has the ultimate responsibility.

One recent event has increased the organisations' focus on cybersecurity substantially, the implementation of GDPR. This will become effective from May 2018 and entail that organisations face major fines if they do not live up to the GDPR decree. This makes the risk of insufficient cybersecurity very tangible – fines up to 4 percent of global revenue or 20 million Euro. This has motivated organisations to get a better hold of their cybersecurity and justified substantial investments in security measures.

> "After May 25th, it is not an option to be indifferent."

For most organisations and companies, the initial focus should be to ensure that basic cybersecurity measures, like backup procedures and ongoing updates and patching of systems, are in place. For smaller companies it is an option to outsource the cybersecurity to an external partner.

In general, the increased level of digitalisation increases the need for protection, and this means that cybersecurity is not a one-off, but an ongoing process. It also means that whenever companies develop new products and services they should take cybersecurity into account as well. Both to ensure that customers' data is safe, but also to keep products operational and functioning.

A simple rule of thumb: if it makes sense to digitalise, it also makes sense to secure the integrity of the digital solution.

3.4. Individuals can be victims themselves, but can also serve as a mean to attack other actors

For individuals, there is a desire to be part of the open network and use all the digital offerings that are available. Furthermore, a world where more objects are connected offers new opportunities and conveniences. However, many individuals also want to protect their privacy and data and have control over what data they share and with whom. For individuals there is a fine line between cybersecurity and data privacy as the two issues are hard to separate.

Most individuals do not know how to deal with the issue of data privacy. For many, they simply do not care too much for data privacy and do not think that they have anything they need to keep private. For others, they find it hard and time consuming to understand and navigate the many rules, settings and solutions while still being able to take part in today's digitalised society. With the increased level of cybercrime and GDPR pushing a data protection agenda, we do expect that individuals will be more concerned with the privacy of their data and raise the demands on companies and organisations who wants access to their data.

Attacks on individuals can happen in their own private sphere – for example if their computer is hacked and breaks down or if their private data is leaked. It is expected that individuals will experience more cyberattacks in the future, as they are generally less protected than companies. Criminals are also known to have tested attacks on individuals before they aim them at companies. Viruses installed on private computers might not be causing any disruption to the computer, why the owner might not notice anything. The virus is inactive but criminals can exploit these for example to form a botnet[12] and attack third-party servers or use processor capacity for mining crypto-currency.

[12] An Internet-connected network of computers infected with malicious software and controlled as a group without the owners' knowledge to create server overload for a third party.

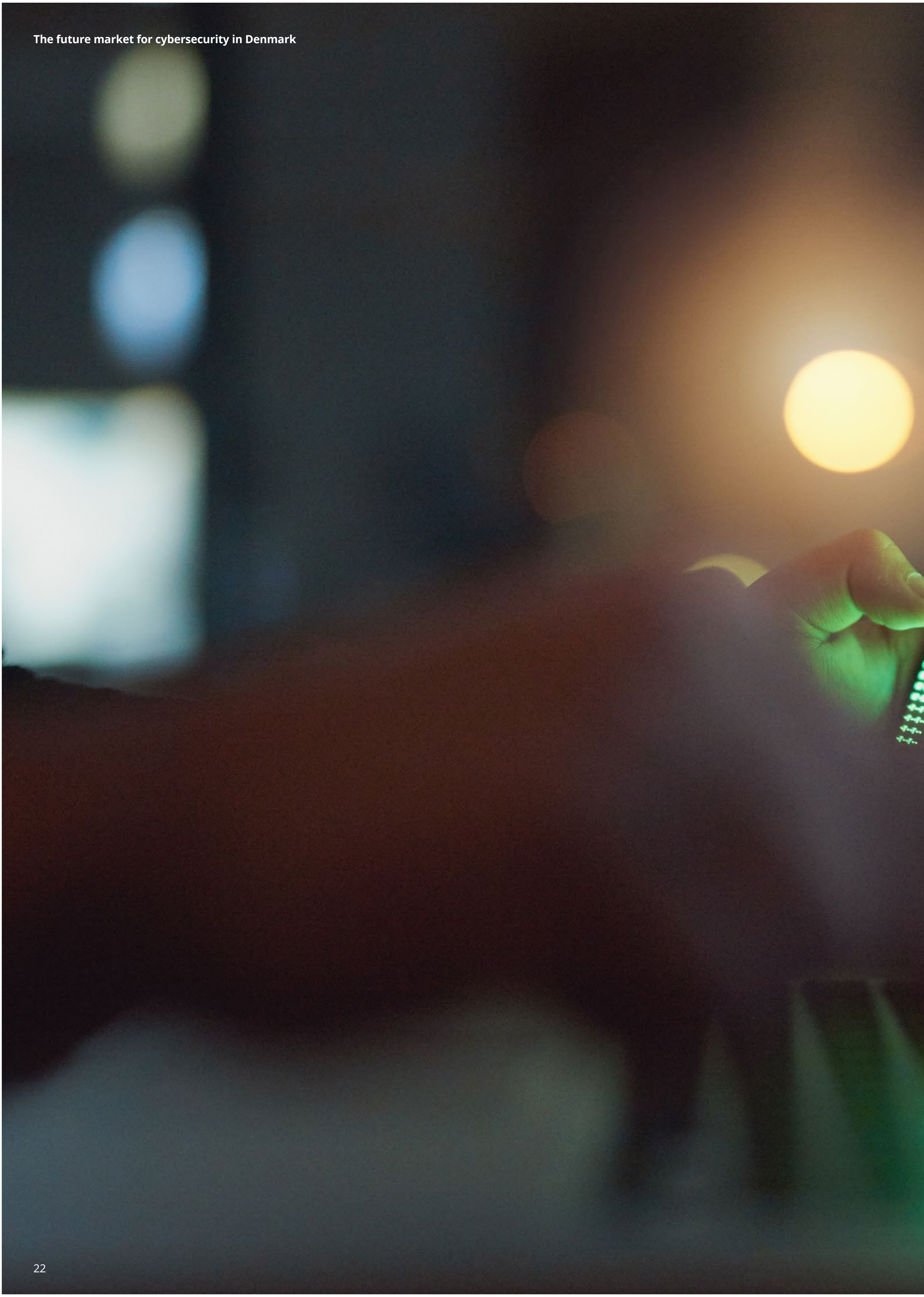
There are many cybersecurity products and services available to individuals to protect their data and computer systems. However, the most important measure will be to raise the level of understanding and awareness about cyberthreats and cybersecurity. This will enable individual consumers to navigate the space of digital products and choose the most secure products as well as demanding them from companies. A general rise in knowledge will not only affect the individuals but will spread to the rest of the victim categories, as individuals are part of all of these.

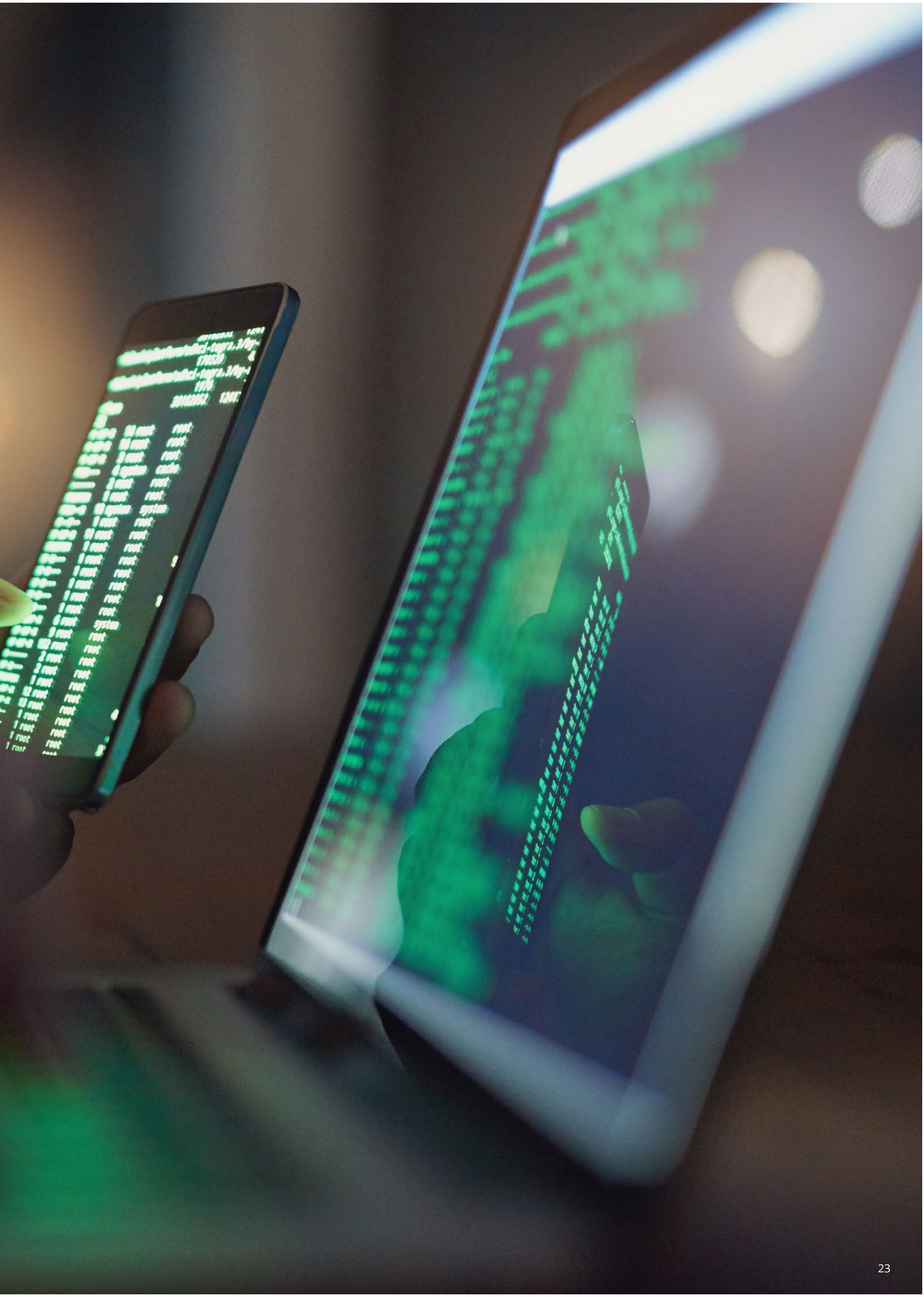
DDOS-attacks from the dorm

In 2016, three young American students managed to build a botnet having an unprecedented size. The code behind the botnet was called “Mirai” and the motive was to move traffic to a specific Minecraft server. The botnet was powered by between 200,000 to 300,000 unsecured Internet of Things (IoT) devices. The young men had built a code that was able to scan the Internet for IoT devices with poor security and then install malware on these devices. The devices were then used to flood servers in so-called DDoS-attacks. Victims included French telecom provider OVH and American tech company Dyn, which is a key provider of internet on the US East coast. Mirai shocked the Internet and some experts thought that the offender was a large nation-state. The Mirai attack shows just how powerful and dangerous IoT devices can be without cybersecurity[13].

”As a country we need to think about what we want to protect. The citizens will to a great extent need to protect themselves.”

[13] https://www.wired.com/story/mirai-botnet-minecraft-scam-brought-down-the-internet/





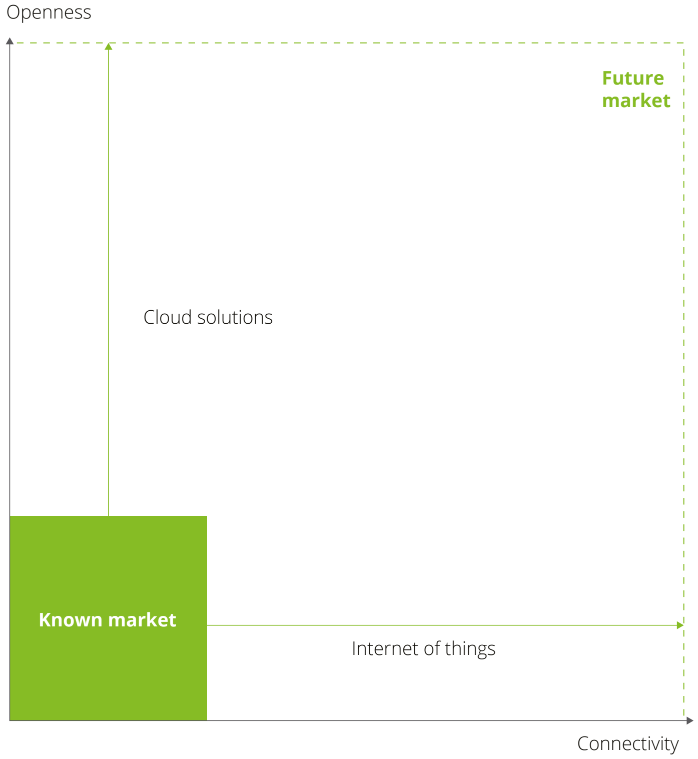
4. What are the business opportunities?

As the cyber-threats spread, the market for cybersecurity grows. The basic dynamic is that awareness drives demand for existing cybersecurity services. On top of the traditional growth, we see two major trends transforming: openness and connectivity, which will further boost the market for cybersecurity.

As described in chapter 3, openness and connectivity are the main advantages of digital solutions. Today, the cybersecurity market is in its infancy and primarily a business-to-business market. In the future, the business-to-consumer aspect will play a much bigger role, either directly as services to consumers or indirectly as a selling point for consumer goods. The cybersecurity agenda will spread to new areas of our daily life – for example cars and technical installations – and bring the agenda closer to the individual consumer.

The current market for cybersecurity services focuses mainly on protecting the perimeter of companies and organisations. This includes preventing offenders from gaining access to servers as well as initiatives to educate employees in behaving correctly in order to prevent breaches and handle them correctly if they do occur. Many companies do this already, but the vast majority of companies is not doing enough. There is a great potential in this emerging market as many actors are underinvesting in cybersecurity. A higher awareness about cybersecurity will thus be a significant growth driver.

Figure 8. Growth drivers



Besides growth in the known market, there will be substantial growth driven by a larger degree of openness and connectivity coming from increased use of technological solutions such as cloud solutions and IoT.

Increased use of cloud solutions will also increase traffic and move it outside the perimeter of an organisation or household. This requires attention to securing traffic. Examples of solutions are encryption of data, monitoring of traffic patterns or shared ledgers, for example in a blockchain.

More devices connected to the Internet (IoT) serve as vulnerability points if they are not adequately secured. Security measures can be added after a product is produced, but the most efficient and secure way to implement security measures into these devices is in the design phase.

Each of these growth drivers will be described in the following three sections:

1. Growth in the known market

2. Growth in cloud solutions driving openness

3. Growth in IoT devices driving connectivity.

4.1. The known cybersecurity market will double in five years

The current market for cybersecurity is primarily driven by known risks related to perimeter protection and user behaviour. This includes services such as:

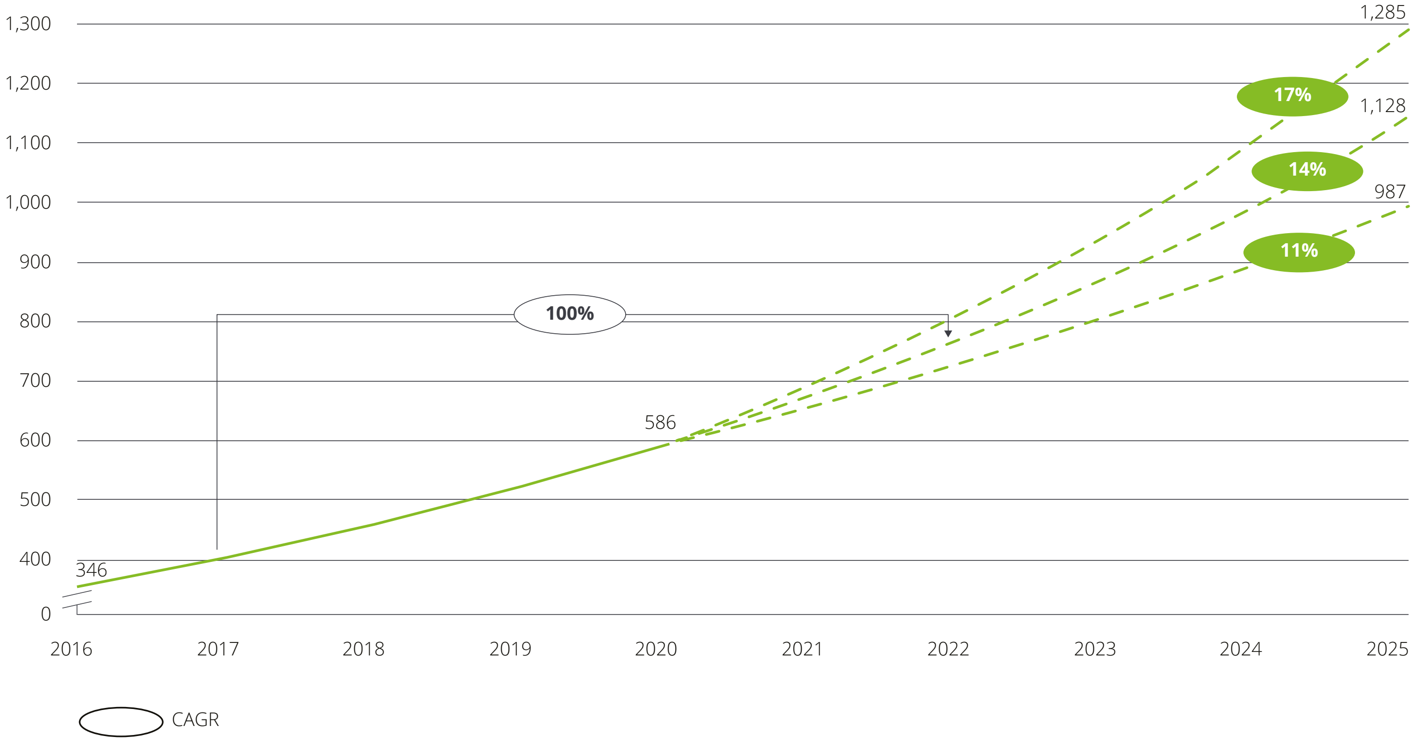
- Filters to identify or stop infected or risky emails
- Virus detection and prevention
- Training of employees to identify security threats and prevent a cyberattack
- Certification of webpages
- Password administration.

These measures are often procured as individual services, but it is also possible to outsource cybersecurity as managed services.

There is still a great market potential in raising cybersecurity measures to a basic level across authorities, companies, organisations and individuals, which drives significant growth in the cybersecurity market we know today. There are different predictions of how much growth the cybersecurity market will experience, but the overarching opinion is that the growth will be dramatic.

Figure 9 illustrates that the known market for cybersecurity in Denmark will double over 4-6 years and reach a level between USD 980m and USD 1300m by 2025. Coming from a current level of around USD 400m in 2017, a doubling or trebling of the level serves as a great growth potential

Figure 9. Cybersecurity market size, Denmark / mUSD



Source: Gartner for Deloitte, Markets and Markets, Mordor Intelligence

4.2. Public attention can drive higher general awareness and thus market growth

Awareness about cybersecurity is low in Denmark. This is one of the reasons why our security level is low. The UN Global Cybersecurity Index is a proxy for the political attention on cybersecurity in a country. We have coupled the index to the current market size for a bundle of European countries to show that there is a correlation between the two, as shown in Figure 10.

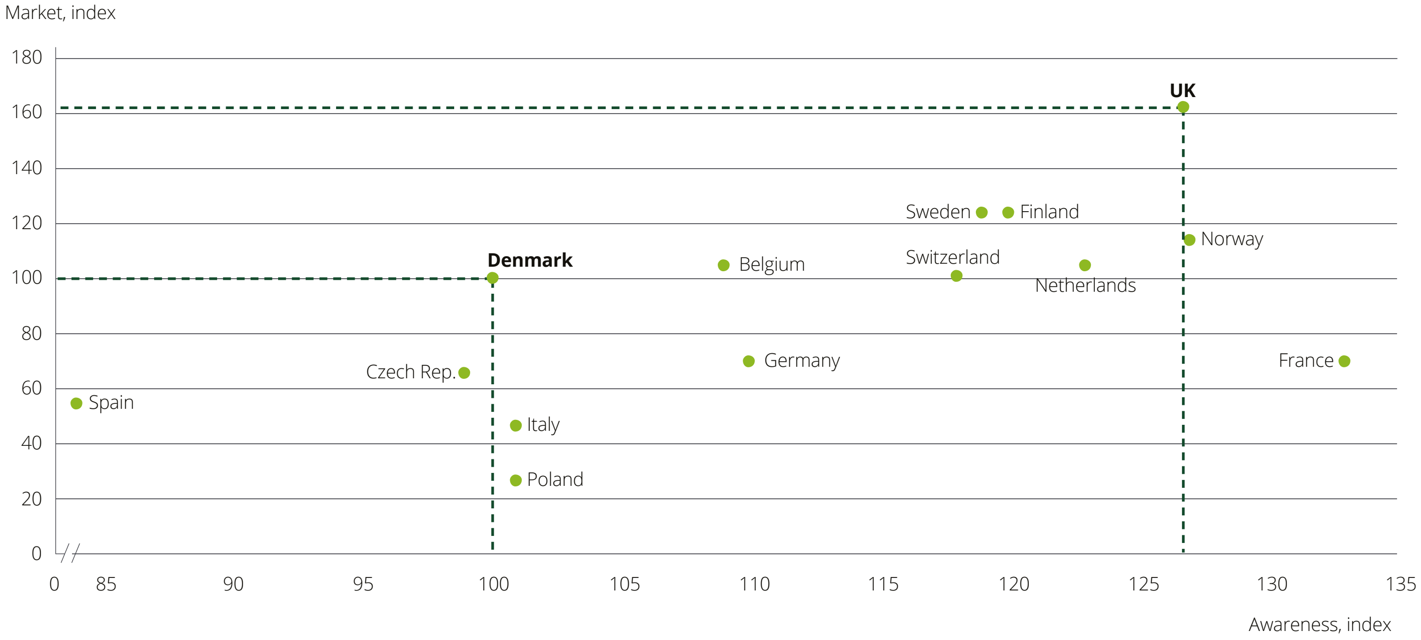
Figure 10 suggests that increased political attention and awareness drive market growth. If Denmark catches up to for example the United Kingdom in terms of political attention and standards, this could increase the market by 60 percent. According to the UN Global Cybersecurity Index, the main areas where Denmark is lagging behind the United Kingdom are related to legal measures on cybercrime, cybersecurity training, cybersecurity standards for organisations and the lack of a homegrown industry[14].

If Denmark improves within these areas, it would contribute to an increased awareness about cybersecurity across the society. Additionally, if awareness is raised among consumers, they will demand improved cybersecurity in the products and services they buy. This would drive companies to embed cybersecurity in their products and services, which could become an important competitive advantage.

> ”There is a much greater awareness in the UK, and more companies are aware of cybersecurity. In Denmark, it is not seen as a business area.”

New political initiatives and regulations are emerging and contributing to increased awareness about cybersecurity. Above all, GDPR will drive increased awareness for authorities and companies as the risk related to non-compliance will grow dramatically, as described earlier. In addition, the recent political settlement of the Danish Defence Policy allocates 1.4 billion Danish kroner specifically to cybersecurity. The size of the allocation in itself emphasises the importance of cybersecurity to the public and the investment will fund a range of initiatives to raise security levels.

Figure 10. UN Index of Cybersecurity Awareness (GCI) plotted against indexed market size / DK=100



Source: Gartner for Deloitte, UN, ITU: Global Cybersecurity Index 2017, IMF GDP growth estimates, Deloitte calculations

[14] It should be noted that the accuracy of the UN Global Cybersecurity Index is disputed in the cybersecurity community as no Danish authority has been involved in the evaluation.

4.3. Cloud solutions create new vulnerabilities and the need for new measures

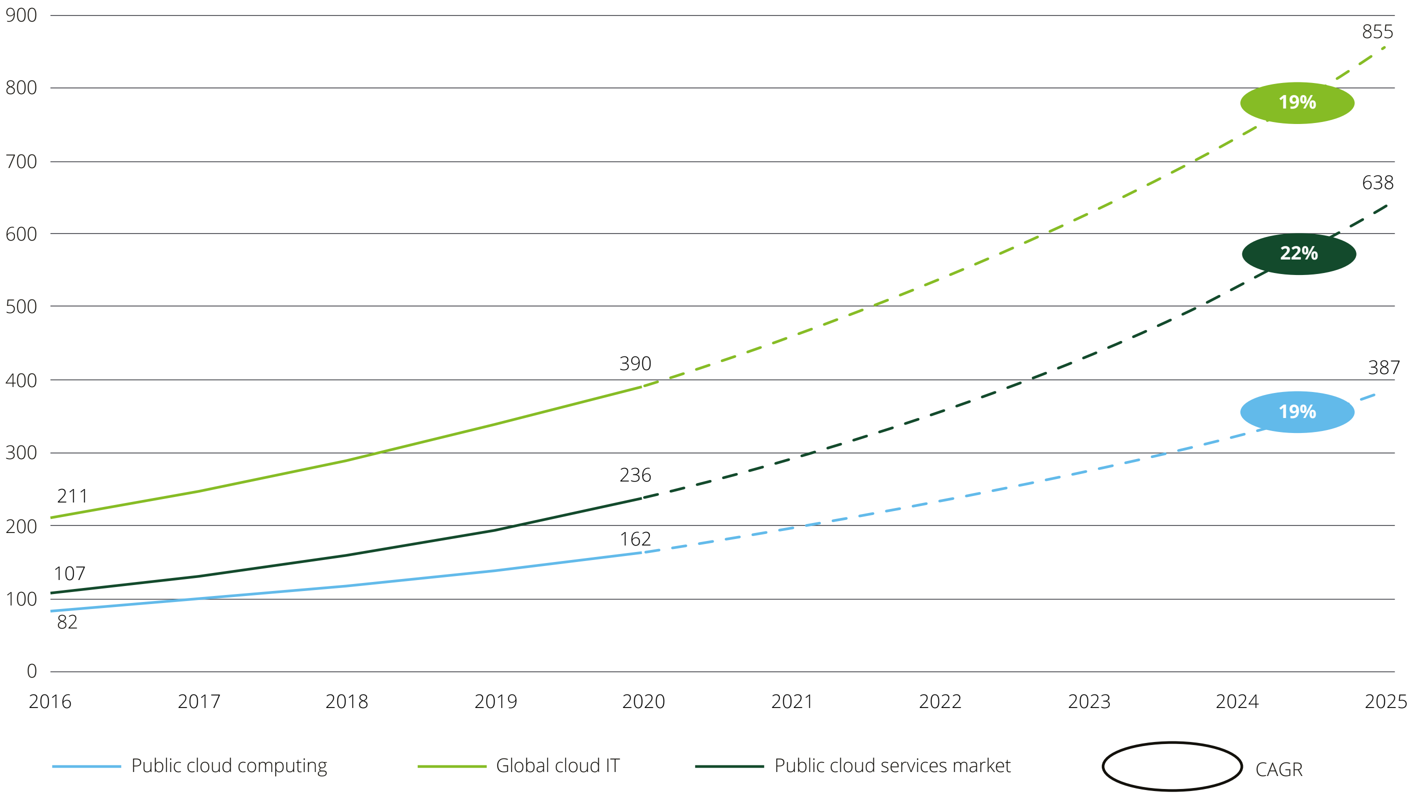
Cloud computing is growing fast and more and more data is stored in the cloud. When data is stored in the cloud, it is no longer enough to secure the perimeter of a company, organisation or household as the external borders are blurred.

The main parameter for security will be safe traffic, for example through encryption, blockchain solutions[15] or AI surveillance of traffic patterns. Even though cloud computing has been around for some time, it is expected to grow significantly in the near future – as shown in Figure 11 – and drive growth within secure traffic solutions. Some of the important growth drivers are faster networks, more connected devices and software and server capacity bought as services.

An increased use of cloud solutions is expected to drive growth in the market for cybersecurity. It is however nearly impossible to guess the size and location of this market. An educated guess is that new or improved applications and services to secure the traffic will compete for dominance in the next 5-10 years.

In Denmark, 38 percent of companies were using cloud computing in 2015[16]. This share is expected to be substantially higher today. If the development follows the growth in Figure 11, this will increase further in the future and create an urgent need for cybersecurity measures in relation to cloud computing.

Figure 11. Cloud computing, global market size / bUSD



Source: IDC, Wikibon, Bain, Gartner, Forrester

[15] The connection between blockchain and bitcoin can make the approach somewhat controversial. However, the potential of blockchain goes far beyond cryptocurrency as illustrated by Maersk's recent investment in a shared ledger for shipping and customs.

[16] OECD "Digital Economy Outlook 2015".

4.4. Digitalisation of products drives the need for security by design

We connect more and more devices to the internet, and IoT is becoming common in productions as well as private households. This development is expected to have great impact on organisations, individuals and authorities as connectivity can optimise everything from production to transport and daily chores.

> ”Manufacturers are not good at thinking about security and privacy when developing products.”

The benefits of IoT are expected to motivate strong growth in a number of connected devices as shown in Figure 12. This development will make companies more vulnerable to cyberattacks, as everyone will become even more dependent on IT and there will be a significant increase in digital entry points. The vulnerabilities will largely be connected to the original design and supply chain for the devices, meaning that security flaws are in the devices by default. A key consideration for manufacturers is therefore to either act fast and implement security by design or wait for future regulation of security.

No matter if manufacturers include cybersecurity in the design of the products or if the consumers add security solutions afterwards, the growth in IoT devices will also drive a growth in the cybersecurity market.

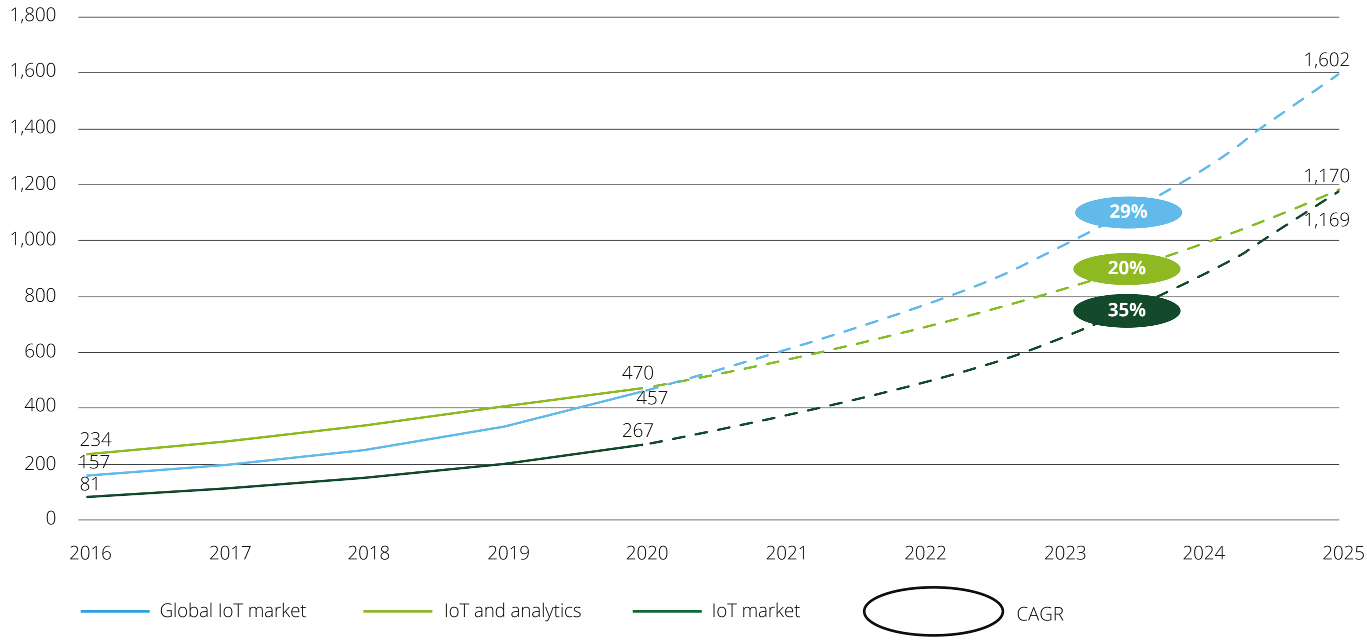
European Union Agency for Network and Information Security (ENISA) is rumoured to prepare standards for cybersecurity in products, but these processes usually take years to materialize and the market will develop in the meantime.

We expect the growth in IoT to drive a similar growth in the market for cybersecurity. However, this growth will take a different shape than the current cybersecurity market and will include new actors and business models.

The starting point for the market development will be end-user needs. Many approaches are possible, but some of the more probable are: new services or features in existing product categories, specific security products to handle security across a range of devices or applications that can secure unsecure products through the network access of a mobile phone.

> ”The Internet of Things is a setback for cybersecurity.”

Figure 12. Internet of Things, global market size / bUSD



Source: GrowthEnabler & Markets and Markets, Bain, BCG

OECD expects all households to have a significant higher number of connected devices by 2022. In 2012, the number of connected devices in an average household was eight. This number is expected to grow to 50 connected devices by 2022 as illustrated in Table 1. The primary categories of future household IoT devices relate to entertainment and building technology.

Table 1. Number of devices per household

2012	2017	2022
8 devices	23 devices	50 devices
• 2 smartphones • 2 laptops/ computers • 1 tablet • 1 DSL/cable/fibre/ Wi-Fi modem • 1 printer/scanner • 1 game console	• 4 smartphones • 2 laptops • 2 tablets • 1 connected television • 2 connected set-top boxes • 1 network-anchored storage • 2 e-Readers • 1 printer/scanner • 1 game console • 1 smart meter • 2 connected stereo systems • 1 energy consumption display • 1 internet-connected car • 1 pair of connected sport shoes • 1 pay-as-you-drive device	• 4 smartphones • 2 laptops • 2 tablets • 3 connected television • 3 connected set-top boxes • 2 e-Readers • 1 printer/scanner • 1 game console • 1 smart meter • 3 connected stereo systems • 1 energy consumption display • 2 connected cars • 7 smart light bulbs • 3 connected sport devices • 5 internet-connected power sockets • 1 connected weight scale • 1 eHealth device • 2 pay-as-you-drive device • 1 intelligent thermostat • 1 network-attached storage • 4 home automation sensors

Source: OECD "Digital Economy Outlook 2015".

4.5. Companies benefit from cybersecurity

Cyber-threats pose a great risk across society. However, there are also great opportunities related to cybersecurity, if Danish companies are able to grasp the growing market. As shown in the above paragraphs, we will see growth in the cybersecurity market as we know it today. As new and better technologies emerge, so will new and different needs for cybersecurity. Both cloud solutions and the use of IoT will cause new needs and demands for cybersecurity measures. As both these markets will see a dramatic growth, we can expect strong growth in the cybersecurity market.

We see three attractive opportunities for Danish companies and start-ups:

- Tap into the growth in the known market and deliver solutions or services.
- Develop new solutions and technologies to secure the increasingly open networks.
- Move first, set the future standard, and claim a competitive advantage from secure connected products.

For the companies who ignore the direct market opportunities, it is an obvious priority for management to ensure a sufficient level of cybersecurity. What is sufficient depends on the organisation, but the right level can be identified in three steps:

1. Establish basic security: All companies need to ensure that they have basic cybersecurity measures in place such as firewalls, antivirus, patching of systems, backup procedures, authentication of users and a basic employee awareness.

> "Start with the basics: Backup, antivirus, firewall and patching. Or get someone to do it for you."

2. Secure digital choices: Additional cybersecurity measures should be balanced with the company's need to protect its systems and data. A high level of digitalisation and high data sensitivity drive a high level of cybersecurity. Data concerning the business as well as data about for example employees, customers or partners should be taken into consideration. The obvious approach is: if it makes sense to digitalise a process, it all also makes sense to secure it.

3. Prepare for the inevitable: Finally, every company should have cybersecurity measures in place to detect any breaches as well as contingency plans in case of a breach. A crucial consideration is if the company has concentrated risk on one or few factors, for example all operations depend on the ability of all employees to log in to one big network.

Cybersecurity entrepreneurs

Uniqkey
Easy and secure access control
An example of a company that provides easy-to-use password management and two-factor authentication for employees in small-sized and medium-sized companies.

The app-based solution makes it easy to administrate all employees' access to cloud services and helps the user log in securely on both professional and private services.

BlackstoneOne
Server updates as a service
Monitors the ongoing development in vulnerabilities and patches for company servers.

Instead of buying occasional security scans, the customer gets daily updates on new vulnerabilities and solutions from all available global sources.

Dencrypt
Useable encryption
Provides advanced and user-friendly encryption solutions for protection of smartphone communication. Users are presented with mobile apps to make encrypted calls as easy to use as traditional phone calls. Among Dencrypt's customers are the Danish Defence and NATO.

> ”There are two types of companies – those who have been hacked and those who do not know they have been hacked.”

4.6. Denmark has the prerequisites to claim a leading position

Denmark could become a frontrunner in the emerging market for cybersecurity, and Danish companies should take advantage of our existing strengths.

Based on our interviews, we have identified these strengths to be:

• High level of digitalisation
- Denmark is one the most digital societies in the world, as shown earlier. This is a vulnerability, but also an asset as all citizens are used to digital solutions.
- It is relatively easy to recruit employees with basic IT skills in Denmark compared to countries that are less digitalised.

• Scientific strengths
- Denmark has a well-developed research environment within cryptography that has led to commercial solutions in companies working within this area. Most experts rank the Danish cryptography community as top 5 in Europe.

- The Danish cybersecurity community also contains knowledge within AI and automated thread seekers, which is instrumental to cybersecurity analytics where traffic data can be used to detect abnormal patterns and threats.

• Advanced identification
- The CPR (central registration of persons) system has been the starting point for early experiences with digital identification with NemID and the coming MitID. The upside is that we have built significant experience in the area. The downside is that we have concentrated our risk and may be slow to adopt more secure opportunities, which is a challenge that for example MitID will have to mitigate.

• Usability
- Danish companies have a tradition for designing products that are intuitive and easy to use. Part of this is a strong design tradition with participatory design and user involvement that is not only focused on making visually appealing products but also use methods from social sciences to improve usability. Usability is an underestimated part of getting users to adopt secure solutions.

• Trust
- Danes are known as trustworthy and trusting people. This culture and image could be used in developing and branding future cybersecurity services and products. Trust is not in itself a good approach to the cybersecurity threats, but solid, usable solutions for the future must be based on our natural inclination to build trusting relations.

These key strengths can differentiate Danish cybersecurity solutions and products on the global market. In Denmark, we are good at working in a cross-disciplinary manner, and in combination, these key strengths have the potential to generate technically strong products that are trustworthy and easy for users to use and implement in their daily lives all over the world.

5. We should focus on competences, network security and security by design

All trends suggest significant growth in the cybersecurity market. Danish companies could benefit from the development and create a global position of strength.

Based on the technological trends and Denmark's key strengths, we have three recommendations for tapping into the potential and creating new business potential:

1.Cybersecurity competences.

2.Secure traffic and networks.

3.Security by design.

5.1. Cybersecurity competences

A high level of competences and awareness will create a more skilled workforce that can serve as a differentiator by itself. It will also create a market pull, as consumers will demand more cybersecurity in the products they purchase. The efforts to grow skills are no different from other educational areas. We suggest the following actions:

> ”We must create a cybersecurity culture.”

> ”We should educate for more data awareness.”

The efforts to grow skills are no different from other educational areas. We suggest the following actions:

- Include cybersecurity in basic education and regulate cybersecurity training requirements for companies and professions.

- Develop national campaigns to push awareness among companies and individuals to increase the understanding of cybersecurity and data privacy. The campaigns should emphasise that cybersecurity is not something you complete but an ongoing process.

- Invest in scientific competences to drive the development of both cybersecurity and the business it generates.

- Increase collaboration across authorities, companies and scientists to combine knowledge, experience and resources and thereby create better cybersecurity solutions.

> ”For Denmark to take a leading position within cybersecurity, we need to raise the standards on all levels. Including our level of knowledge.”

Almost every Danish company is connected to the internet. Even for the smallest companies, more than 98 percent have a broadband connection. This suggests that virtually everyone is interacting with the internet in some way and this spreads the risk. This emphasises the need to ensure a basic level of cybersecurity awareness and knowledge.

Broadband connectivity in Danish companies, 2010 and 2014

87%	99%
2010	2014

Source: OECD “Digital Economy Outlook 2015”.

> ”We need consumers to demand better products. This can drive the right development and increase competition within the field.”

Next steps?
The above recommendations can be put into practice in several ways. We suggest to:

- Teach cybersecurity in primary schools. This can be done by having a cybersecurity theme as part of the education in computational thinking as these two subjects are related.
- Guide companies towards educating people who have tasks that are related to managing data or systems on cybersecurity, including contingency plans in case of a breach.
- Develop specialised cybersecurity education as part of professional training for professions that include handling of personal data or navigation in complex systems, for example nursing or shipping.
- Set a goal for the number of students that should take a specialised cybersecurity education and create incentives for the universities to reach this number.
- Create deeper knowledge within cybersecurity by investing more resources in public research and innovation within:
  - Identity and access management
  - Trustworthy computing
  - Network security
  - Cryptology
  - Security in socio-technical systems
- Establish targeted and strong public-private partnerships that include authorities, companies and research institutions, for example anonymised learnings from GDPR incidents and threat intelligence.

The table (to the right) suggests more detailed recommendations for scientific areas that are worth investing in.

> “The scientific community is small. Less than 20 scholars are permanently employed at Danish universities.”

Identity and access management	• Identification (including national electronic id systems) • Authentication (including biometrics) • Privacy by design (including privacy enhancing technologies, attribute-based credentials and zero-knowledge protocols) • Access control policies and mechanisms.
Trustworthy computing	• Security by design (including security engineering and programme/protocol security) especially in relation to Internet of Things • Computational trust and trust management systems • Autonomous component security (defence in depth).
Network security	• Intrusion detection systems (including detection of malware/botnet/exfiltration/ etc.) • Anomaly detection systems • Security through decentralisation and shared ledgers, for example blockchain.
Cryptology	• Light weight cryptology • Quantum and Post-quantum cryptology • Secure multi-party computation • Security of critical systems.
Security in socio-technical systems	• Security and the law • Security usability • Data ethics and social acceptability, for example personal data in research.

5.2. Secure traffic and networks

Today, the focus is mainly on securing the perimeter, but as we move more activity outside the perimeter and into the cloud, perimeter protection will not be enough. We therefore need to increase focus on securing the traffic and be able to detect breaches and have contingency plans in place for breaches in open networks.

> "Our researchers are especially good at cryptology."

This can be done by focusing on the following:

- Utilising and expanding our scientific expertise as described in detail in 5.1
- Building national standards and solutions to secure data in open networks to stimulate further development
- Combining technical expertise with sociological methods to create user-friendly solutions.

> "It is necessary to match cybersecurity with how people work – this is what the hackers do with social engineering. And they are good at it."

Denmark is the most digitalised country in Europe and therefore serves as a great "lab" in which to test new cybersecurity solutions. Danes are comfortable with digitalised products and services and, at the same time, sensitive consumers. We expect interfaces to be attractive as well as easy to use.

Denmark is the most digitalised country in the EU (DESI score[17])

0.71	0.53
DK	EU

Next steps?

Denmark has a strong scientific tradition within cybersecurity, but we need to invest and set high ambitions for science and technology as well as commercialisation to claim a leading position in the market. We suggest the following initiatives:

- Take advantage of the strong competence bases that Denmark has within cryptography to create new product offerings and support further scientific research and development.
- Increase national traffic monitoring, for example through AI, as we cannot ensure that no unwanted traffic will cross the perimeter, and it is necessary to monitor abnormal patterns to identify breaches.
- Secure network traffic through improved identification of sender and receiver. We currently use NemID, and MitID is on the way. Other countries, for example Austria, set very high standards for identification methods.
- Increase awareness about breaches happening to incite development of contingency plans.

> "There is a tendency to design security as magic – something that is not understandable. That requires faith."

- Stimulate shared ledgers, for example blockchain solutions, to secure traffic and data validity across many independent actors.
- Develop security solutions for operational technology, for example in relation to critical infrastructure.
- Focus on creating user-friendly solutions to ensure easy usage. Danish companies are good at creating user-friendly products. This legacy can be utilised in new cybersecurity products and solutions. One approach could be to involve the Danish Consumer Council in the development and testing of digital solutions.
- Recognise the human aspect in cybersecurity as an advantage and design products made for the human mindset and knowledge span – rather than hoping for fundamental changes to human nature.
- Use Denmark as a laboratory to test solutions.

[17] DESI is a Digital Economy and Society Index. The DESI score is based on connectivity, human capital/digital skills, use of internet by citizens, integration of digital technology by businesses, and digital public services

5.3. Security by design

Many products and services lack cybersecurity measures from the beginning, which increases the vulnerability to cyberattacks. It is possible to add cybersecurity measures after production, but this is difficult and often less efficient.

We should therefore develop a new manufacturing tradition based on security by design by taking the following actions:

- Create national standards and certifications to invoke clear incentives for companies to implement cybersecurity measures and allow for more tangible business cases. This will bring Danish companies to the front of the race for the future solutions and push the need for international standards in the future.
- Develop best practices in different industries and guidelines for implementing cybersecurity measures to companies with no or limited levels of cybersecurity. The best practice for a farmer is not the same as the best practice for a bank.
- Promote security by design among Danish manufacturing companies to stimulate secure technological products.
- Utilise the interface development competences residing in the Danish design community to ease development and design processes as well as making security by design more appealing to companies and consumers.

> "Cybersecurity is a precondition for growth and optimisation."

According to OECD, Denmark ranks second in the number of online devices per 100 inhabitants with 32.7 online devices per 100 inhabitants in 2015. As a result, Denmark is highly vulnerable in terms of IoT devices with low levels of cybersecurity. Regulation is necessary to bring down the risk and stimulate market development.

Devices online per 100 inhabitants, 2015

32.7	23.0
Denmark	Average of top 12 OECD countries

Source: OECD "Digital Economy Outlook 2015".

> "Investments in cybersecurity are a cost that affects competitiveness. If the same rules apply to everyone, we are playing on the same field."

> "If we had a certification system, it would increase independence. You would have a third party validating the level of cybersecurity."

Next steps?

To increase the level of security in connected devices, we suggest developing a set of standards that can guide companies on how to include security in their product development. The key to implementing security by design is to include cybersecurity measures in the product from the beginning. This will make them secure by default and enable more advanced security measures. Such development can be stimulated by a national certificate (that may later become international) based on a set of guidelines. These guidelines could require that device manufacturers:

- Enable changes of passwords or more advanced identification technologies.
- Make it mandatory to change default settings. For example, the device keeps suggesting a change of password until the user has carried it out.
- Implement automatic update of software or application management solutions.
- Account for the origin of elements in a solution, for example sensors, cameras and software, to increase transparency in the product design and make tracking of vulnerabilities possible and thereby create a greater sense of responsibility in all parts of the supply chain.

It is important to note that the above suggestions are very general and that the needed cybersecurity measures will vary between different products and industries. Therefore, it can be beneficial to create industry specific standards.

6. Cybersecurity vocabulary

6.1. Motive

One or more of the following ambitions can motivate a cyberattack.

Economic gain
Causing a cybersecurity breach for economic gain, for example from ransom or from getting credit card information.

Activism
Intention of sharing a message with a large group or stop an activity that the offender oppose.

Espionage
Getting access to confidential information or intelligence.

Vandalism
Merely a purpose of causing harm without any gain.

Terror
Causing death, destruction, or loss of control through digital breakdowns.

Misinformation/fake news
Spreading wrong or skewed information.

6.2. Offender

The offender can be different types of organisations or individuals.

Individuals
An individual without any affiliation to the victim, other criminals or other entities.

Internal employees
A cybersecurity breach can be due to intentional actions from an employee who deliberately wants to cause harm. These should not be mistaken for an employee that unintentionally causes a cybersecurity breach, for example by clicking on a phishing mail.

Organised criminals
Criminals who run an illegal business performing cybercrime to their own benefit or sell cyberattacks as a service on the black market.

Companies
Companies who want to harm a competitor or get access to confidential information.

States and governments
States or national entities can be behind the cybersecurity attacks, for example to get or spread information or shut down infrastructure or weapon systems.

Terror groups
Terrorists who use digital means to harm their opponents.

6.3. Security threats

The offender can use different tactics to threat the victim.

Manipulation
When an offender manipulates an individual to a specific action that will cause a cyberattack. Sub-categories are:

- Phishing: An attempt to manipulate a person into passing on sensitive information or click on infected links. Phishing mails are often sent to many recipients at the same time.
- Smishing: Phishing through text messages.
- Social engineering: The victim is manipulated to conduct an action or pass on classified information without knowing it. To be effective, social engineering requires some knowledge about the victim.
- Business Email Compromise (BEC): Also known as CEO fraud. The offender makes credible, targeted emails where they pretend to be for example the CEO and get the victim to act as they received an order from the management, for example by transferring money to an account.
- Credential harvesting: Redirecting the victim to a fake login-page to get the victim’s account information.

Malicious installations
Software installed on a victim’s server that performs unwanted actions – widely referred to as ‘virus’. The most fundamental terminology includes:

- Malware: An umbrella term for different types of malicious software, such as adware, ransomware and spyware.
- Adware: Type of software that shows advertisement to the user.
- Ransomware: Type of software installed on a computer that blocks access to IT-systems and data until a ransom is paid.
- Spyware: Type of software installed on a computer to collect personal information and track the user’s internet activities.

Hacking
Hacking is unauthorised intrusion into a computer or network and thereby viewing, copying or creating data without the intention to destroy data:

- Targeted intrusion: A hacking action targeting a specific victim.
- Opportunistic targeting: A hacking action targeting a large number of victims by taking advantage of general vulnerabilities.
- Exploits: A software tool designed to take advantage of a flaw or vulnerability in a system.

Server overload
A server is not able to handle all incoming requests:

- (Distributed Denial of Service) DDoS attack: An attack where multiple compromised computer systems are used to attack a target, for example a server or a webpage, in order to cause denial of service for the intended users of the target.
- Botnet: An Internet-connected network of computers infected with malicious software and controlled as a group without the owners' knowledge to create server overload for a third party.

6.4. Infrastructure

The arena where the threats materialise. It consists of the channels where both offenders and victims operate and the vectors used for a cybersecurity attack.

Channels

The digital or analogue platforms where offender and victim meet:

Network

- Internet: When websites are used as a channel to transfer a cybersecurity threat, for example malicious software.
- Infrastructure: For example telephone networks or traffic regulation systems can be used as a channel for a cybersecurity attack.
- Wireless networks: Any form of wireless connection (for example WiFi and Bluetooth) that can be open for cybersecurity threats.

Devices

- PCs and servers: The computers, laptops and servers we use for daily work can be deployed as a channel for a cyberattack.
- Mobile devices: Mobile telephone services can be used as a way to channel a cybersecurity attack, for example through SMS or Snapchat.
- Servers: Access point for a cybersecurity attack e.g. via email.
- Autonomous devices: With the rise of autonomous devices such as autonomous cars and drones these can be hacked and used for unintended purposes.
- Robots: Robot and automation used to automate production and reduce the need of human resources. The control systems can be an entry point for an entity in a cybersecurity attack.
- Internet of Things (IoT): IoT is a network of devices/objects with different instalments that allows the objects to connect and exchange data. These networks can transfer a cybersecurity threat.
- Supply chain: Getting cybersecurity threats into the organisation through a supplier even through products or by having interlinked systems.

Applications

- Software: Programs installed on the devices that can be vulnerable to attacks.

Behaviour

- Employees: Insiders in a company or organisation can be used as a channel to initiate a cybersecurity breach, for example if they are bribed by an outsider.

Vectors

The mean used to execute the cybersecurity attack:

- Emails: Emails can be used as a vector for example by sending a link that when clicked on initiates a malicious installation.
- Remote Command Execution: When an offender can get remote access to a server.
- Watering hole: A third-party webpage is infected with malware that harvests data from the webpage or transfers the users to a webpage controlled by the offender.
- Physical devices: When a physical device is used for a cybersecurity attack, for example a USB key or an IoT device.

6.5. Security measures

The measures a potential target can rely on to protect their data and IT-systems against cybersecurity attacks. The general focus is on protecting the perimeter – the outer 'wall' of an organisation – but security measures also include activities in the outside network and human activity before and after a breach. To grasp that, we look at four categories: Networks, devices, applications and behaviour. The current focus are on the last two.

Network

- Traffic monitoring: Monitoring traffic in the network to identify abnormal behaviour or unwanted traffic.

- Encryption of files and data: Encoding a file or data through an algorithm to prevent unauthorised parties to get access.

Devices

- Access control: The ability to secure access to a device and changing default passwords.

- Security updates: Changing security settings and updating to new standards.

- Safe sensors/supply chain: Knowing the history or suppliers of products to ensure security in all components.

Applications

- Firewalls: Set of related programmes that protects the programmes of a private network by preventing users of other networks from gaining access.

- Antivirus: A software designed to detect and destroy computer viruses. A computer virus is a malicious software programme that loads onto a computer without the user's knowledge and performs malicious actions. As a biological virus, it can spread from one computer system to another.

- Patching: 'Mending' holes in a computer programme. Piece of software designed to fix a security vulnerability and other bugs in a computer programme.

- Backup: Process of copying files and/or data that can be used to restore files if these are lost or damaged in any way.

- Monitoring: Monitoring activity on a computer to detect if any unwanted actions and behaviour is carried out.

- Computer logging: Tracking events that occur in an operating system to identify unwanted activity.

- Spam/mail filters: Software that processes incoming emails and detects unwanted content to prevent it from reaching the mailbox.

- Blocking: Internet filter that blocks offensive or unwanted websites

- Analyses and tests: Analysing and testing the defence and security measures of a cybersecurity to detect vulnerabilities and holes.

- Documentation: Documenting critical IT-systems and data to identify what is most critical for the entity and aligning the security measures accordingly.

Behaviour

- Training of employees: Formal and structured training of employees regarding cybersecurity, typically covering awareness about potential cybersecurity threats and expected behaviour when facing unknown sources of information.

- Analyses and tests: Analysing and testing the defence and security measures of a cybersecurity to detect vulnerabilities and holes.

- Documentation: Documenting critical IT-systems and data to identify what is most critical for the entity and aligning the security measures accordingly.

- ISO-standards: International standards that specifies good practice in a certain area. For cybersecurity, the ISO27001 sets the common standard for good information security.

- Procedures: Having a policy on how to act when using IT to avoid breaches as well as having a clear contingency plan in case of a cybersecurity breach in order to limit harm and impact.

- Strategic considerations: Apart from direct security measures, a strategic framework for cybersecurity should include governance, resilience and vigilance. Governance is the structures and rules an organisation puts in place to control all other measures. Resilience is the measures to deal with the cybersecurity attack when it is in progress. Vigilance is the ability to detect and understand coming cybersecurity threats.

6.6. Victim

Potential targets for cybersecurity attacks fall in four categories. They are interconnected in the sense that an attack on one type of victim can affect the others.

Authorities

All public authorities that can be harmed by a cybersecurity breach, for example by having data and information on citizens leaked or by losing control over a system. A cybersecurity breach on authorities can have an indirect impact on companies and organisations as well as individuals and may fundamentally challenge the position of the authority.

Network and Information System (NIS) companies
NIS companies is a category defined by EU regulation[18]. They include operators of essential services and include both public and private entities. These companies are within energy, transport, banking, financial market infrastructures, health sector, drinking water supply, digital infrastructure and digital services. A cybersecurity breach on these type of companies can have a big impact on society, including other organisations and individuals.

Other companies and organisations
All types of organisations can be harmed by a cybersecurity breach, for example from a breakdown in their IT-systems or by having crucial data leaked. These organisations can be all type of companies, for example a production company or a charitable organisation.

A cybersecurity breach primarily affects the organisation but can also hit individual customers or users related to the organisation.

Individuals
All citizens can experience a cybersecurity attack in their private life. They may also be affected by cybersecurity breaches happening at for example authorities, NIS companies or other organisations.

6.7. Effect

When analysing cybersecurity we distinguish between three levels of effect:

Attack
An offender tries to harm a victim but do not necessarily succeed. An attack will often be blocked by security measures on devices and applications that are in place to prevent intruders from entering.

Breach
The attack breaks the security measures but do not necessarily harm the victim. Harm will often be prevented by actions taken by people after the breach to limit the effects from the attack. This can for instance be having a good contingency plan that can be implemented quickly.

Harm
The breach causes a loss for the organisation, for example of data or money.

Overview of interviews
- David Nyrop, COO/Partner, *Blackstoneone*
- Torben Pryds Petersen,CTO, *Cryptomathic*
- Morten Rosted Vang, IT safety expert, *Dansk Industri*
- Christian Damsgaard Jensen, Associate Professor, *DTU Compute*
- Ebbe Skak Larsen, Security Lead Architect, *KMD*
- Jakob Illeborg Pagter, CTO, *Sepior Aps*
- René Rydhof Hansen, Associate Professor, *AAU – Institute for Computer Science*
- Jens Myrup, Associate Professor, *AAU – Institute for Electronic Systems*
- Kim Høse Jensen, Security Director, *Atea*
- David Simonsen, CEO, *DenCrypt*
- Hakan Yagci and Mattias Fjellvang, Founders and owners, *UniqKey*
- Henrik Ejby Bidstrup, Head of Department, *ITU*
- Michael Stübert Berger, Associate Professor, *DTU Photonics*
- Irina Shklovski, Søren Debois, & Carsten Schürmann Associate Professors, *ITU*
- Niels Zibrandtsen, CEO, *Zibra*
- Mads Nielsen, Professor, Head of Department, *DTU Computer Science*
- Janne Glæsel, Partner, *Nyborg og Rørdam*
- Henrik Udsen, Professor, *KU Law*
- Anja Bechmann, Associate Professor, *Aarhus Institute of Advanced Sciences*
- Ole Lehrmann, CEO, *Alexandra Instituttet*
- Jens Christian Godskesen, Pro-rector, *ITU*
- Thomas Lund-Sørensen, Director, *Center for Cybersikkerhed (CFCS)*

Workshop participants
Agrointelli - B&O - BEC
Cobham SATCOM - Conscia
COWI - Cryptomathic
Dansk Industri - Dansk Ingeniør Service
Erhvervsstyrelsen - IT-brancheforeningen
Krifa - Københavns Kommune
LEGO - MADE - NRGI - Politiet
Sygesikring Danmark - Systematic
Tryg - Tænk - UAS Denmark

[18] EU directive 2016/1148

About the authors

Innovation Fund Denmark: Peter Høngaard Andersen, Managing Director. Tore Duvold, Executive Vice President. Michael Adsetts Edberg Hansen, Senior Scientific Officer and Investment Manager.
Alexandra Institute: Ole Lehrmann Madsen, Managing Director. Gert Læssøe Mikkelsen, Head of Security Lab. Laura Lynggaard Nielsen, Specialist Anthropologist.
Deloitte: Michael Hjortlund, Partner, Monitor Deloitte. Lars Syberg, Partner, Risk Advisory. Erik Lind Olsen, Director, Small Great Nation. Carina Jensen, Consultant, Monitor Deloitte.

Acknowledgements

The authors are grateful for the support of the many organisations and individuals who have contributed to the report (see 6.2 and 6.3). Especially we would like to thank the Steering Committee: Flemming Besenbacher (Innovation Fund Denmark), Thomas Lund-Sørensen (Danish Centre for Cybersecurity), Jens Christian Godskesen (ITU), Christian Damsgaard Jensen (DTU Compute) and Morten Rosted Vang (DI).

About the three partners

Deloitte provides audit & assurance, consulting, financial advisory, risk advisory, tax and related services to public and private clients spanning multiple industries. Deloitte serves four out of five Fortune Global 500® companies through a globally connected network of member firms in more than 150 countries and territories bringing world-class capabilities, insights and service to address clients' most complex business challenges. To learn more about how Deloitte's approximately 264,000 professionals make an impact that matters, please connect with us on Facebook, LinkedIn, or Twitter.

Innovation Fund Denmark provides public investments for developing cutting edge research and innovative solutions. Our aim is to create growth and employment and to solve societal challenges by moving Denmark to the forefront of Science and Innovation. We are ready to invest, where others might not yet be ready to run the risk. Cyber Security is a focus area for Innovation Fund Denmark with investments in cyber-physical systems and digitalization projects, where security is pivotal for success.
In 2018, the budget of Innovation Fund Denmark is 1.4 billion DKK.

The Alexandra Institute helps public and private organisations apply cutting-edge IT research and technology. We are a non-profit company with a mission to create value, growth and welfare in Denmark through IT-based products and services. Our team of specialists design novel, innovative IT-based products and services. We apply our skills in software, user involvement and innovation methods to create technological solutions of commercial relevance with the aim of helping companies boost their business.

Deloitte.