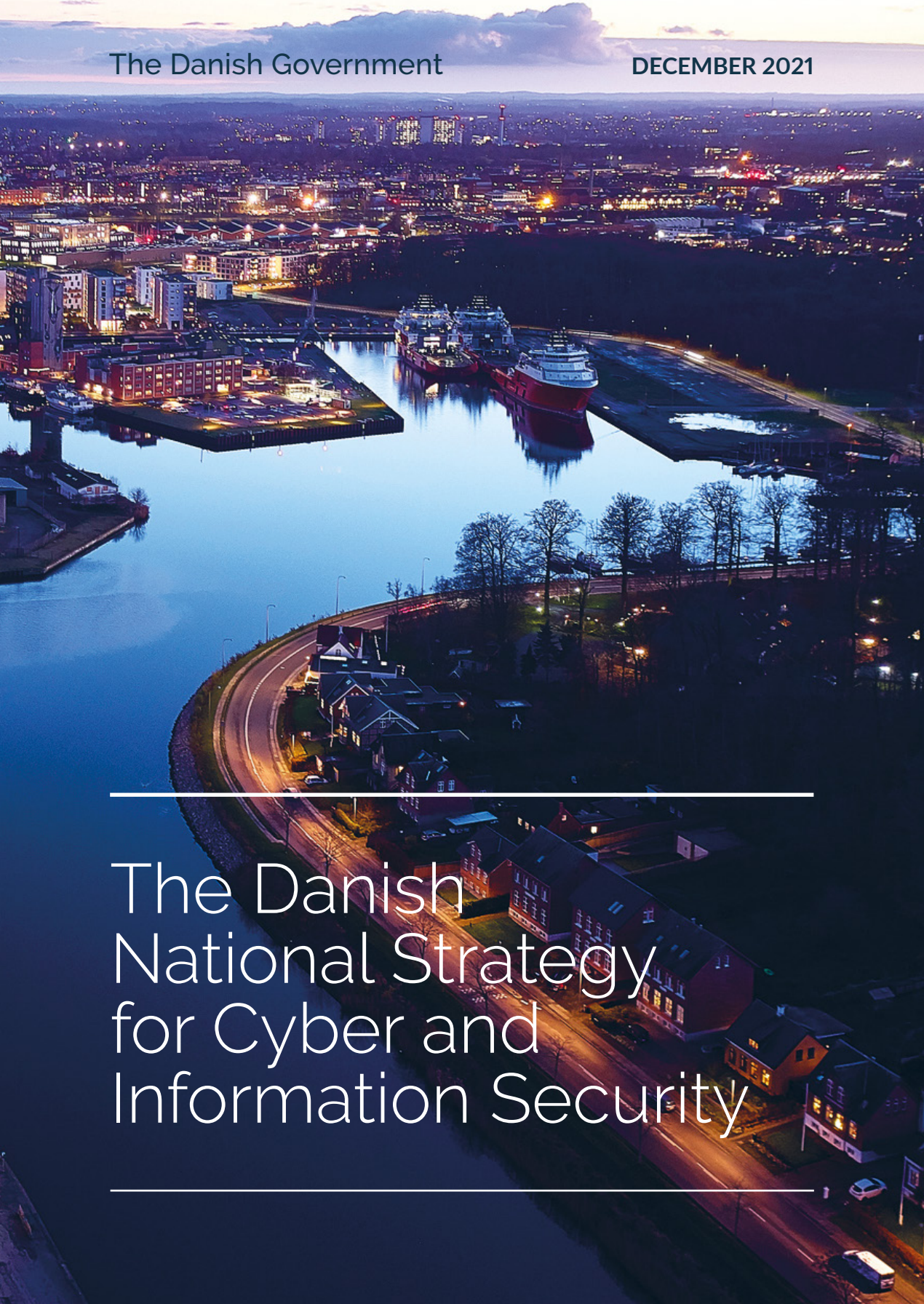
The Danish Government

DECEMBER 2021



The Danish National Strategy for Cyber and Information Security

Contents

Preface

Denmark is one of the world's leading countries when it comes to digitisation. Daily life in Denmark is digitised, whether in private life, at work, or in encounters with the Danish public sector.

Digitisation is a key driver for the development of Danish society. New opportunities for economic growth and increased prosperity come with technological progress. However, the high level of digitisation does also include increased vulnerability with criminals trying to exploit the vulnerabilities of our digital society.

The cyber threat is one of the most serious threats against Denmark. This threat has become a basic condition to which we must all adhere to in our private lives, in our working lives and in society as a whole.

Every day, our public sector, businesses and citizens are a target of large or small-scale cyberattacks. Hackers, criminals and hostile intelligence services put the digital security of people in Denmark under pressure. The Danish government takes this threat very seriously.

Denmark already has a solid foundation to meet the challenges. The Danish citizens generally have a strong digital understanding, and ICT security has for many years been a focus area for many companies. In the public sector, decades of focused efforts from the public side to promote digitisation in Denmark have given us a well-developed foundation.

However, digital developments are evolving fast, and new forms of cyberattacks are emerging at the same pace. The cyber threat is constantly changing. Thus, a more concentrated effort is needed to keep up with and be at the forefront to meet developments in threats and digital vulnerabilities. This is why the government is now launching a new Danish National Strategy for Cyber and Information Security 2022-2024.

The strategy focuses on government and critical infrastructure, as well as citizens and businesses. External cyber threats demand a joint effort if we are to protect Denmark from malicious cybercrime and cyber espionage.

The Danish government has already agreed with a majority in Parliament to strengthen Denmark's cyber defense by DKK 500 million through the implementation of the political agreement on the cyber reserve. Municipalities and regions are also continuously working to strengthen cyber and information security.

The Danish National Strategy for Cyber and Information Security will further strengthen Denmark's cyber and security with a number of new initiatives that will tie the overall effort together. With this strategy, the government is allocating a total of DKK 270 million to 34 new key initiatives that will equip us to keep the cyber threat at bay and help Denmark be digitally secure – also in the future.

The threat we face is constantly changing and requires public authorities, businesses, and citizens to continuously participate and take active responsibility. Cyber security is a continuous process. Hackers, criminals and cyber spies are constantly challenging our security with new and more advanced methods of attack. With the Danish National Strategy for Cyber and Information Security, we are taking an important step towards increased joint efforts and strengthening our defences against cyber threats, which today constitutes one of the greatest threats to Denmark and Danish society.

/The Danish Government

A significant and complex cyber threat in constant change

The threat from cybercrime and cyber-espionage is considered very high and is expected to remain so in the future. Foreign states and criminal hackers are working systematically, persistently and purposefully to hit carefully selected targets in Denmark. They are continuously trying to abuse the digitisation of our society to spy, commit crimes, undermine democratic processes, and ultimately to perpetrate potentially destructive cyberattacks against Denmark.

The digital infrastructure is increasingly more vital to the functioning of our society. As the society becomes increasingly connected via digital solutions, the amount of digitally transferred information and data increases. In turn, the consequences of breakdown or attack will grow. The cyberattacks of recent years against the Irish health care service and the oil and food industries in the US, among others, clearly demonstrate some of the consequences such attacks can have on a country's ability and capacity to maintain vital societal functions.

Cybercrime is a highly profitable industry at present. The criminals are skilled, professional and driven by the opportunities to gain profit. They adapt quickly when profit opportunities arise, when new tools are developed, or when external circumstances change their business landscape.

At the same time, the threat from espionage by the intelligence activities of foreign states has become more pronounced. Foreign state intelligence services use technological advances and make use of sophisticated hacker groups who, through cyberattacks, are able to compromise and gain access to ICT systems to conduct intelligence operations against Denmark. The intelligence activities of certain states are used to steal valuable knowhow from both Denmark and our allies. Attacks are often complex, and politicians, officials and authorities, as well as research institutions and companies, can be included as either targets or means in these activities.

Denmark is an attractive target for cyberattacks due to our active role internationally, in increased globalisation and international competition. Digitisation and the general openness of society, as well as a high level of technological knowledge, make Denmark an attractive target for cyberattacks.

Likewise, Denmark's active international role attracts both desired and unwanted attention.

Simultaneously, new digital opportunities, such as artificial intelligence, big data, quantum technology and 5G are on the horizon. This puts high demands on how we as a society protect valuable information and the digital infrastructure that is so crucial for the maintenance of our vital societal functions. It also places demands on the companies that are part of our supply chains.

Every day, cyber criminals and spies attack Denmark to blackmail Danish companies, authorities and citizens in order to steal our business secrets that ensure Denmark's prosperity, and to reveal and challenge details of our security and foreign policy to harm Denmark and Danish interests.

Most cyberattacks are averted thanks to advanced technology as well as informed and vigilant public authorities, companies and citizens. However, things do go wrong from time to time, and there are too many security gaps today, which could potentially be discovered by hackers and cyber criminals.

Just as many people do not install home security systems until after they have been robbed, many cyberattacks succeed due to cyber security negligence because of overlooked or downgraded cyber security, which is only prioritised once the damage is done. The hackers have far from won the battle for the digital domain, but the work of making Denmark digitally secure is more important and more urgent than ever.

> Digitisation and the general openness of society make Denmark an attractive target for cyberattacks

The Centre for Cyber Security's key assessment of the cyber threat against Denmark

The threat from cybercrime: VERY HIGH

Cybercrime poses a real and persistent threat to all Danish public authorities, private companies and citizens. The ability of cyber criminals to develop and adapt their tactics to new realities and the specialized cooperation that takes place on closed Internet forums increases the threat.

The threat from cyber espionage: VERY HIGH

The Centre for Cyber Security assesses that foreign states can and will try to steal valuable information from Denmark. Time after time, specific incidents and attempts to attack have given credence to this assessment.

The threat from destructive cyberattacks: LOW

The Centre for Cyber Security assesses that the threat from destructive cyberattacks against Danish public authorities and private companies is LOW. Though several foreign states have the capabilities to launch destructive cyberattacks, they are currently less likely intent on conducting destructive cyberattacks against Danish targets.

The threat of cyber activism: LOW

The numerous protests seen in 2020 have not been reflected in more cyber activism attacks worldwide. The number of attacks has thus remained at the same level as in previous years.

A cyber and information security boost in Denmark

The efforts made so far to ensure a high level of cyber and information security have increased a maturity across society. There is a greater awareness and attention to the area. Cyber security has been strengthened in the state and in six designated critical sectors (energy, health, transport, telecoms, finance and maritime) with the establishment of decentralised cyber and information security units (DCIS) and targeted strategies. In addition, government agencies are required to follow the international management standard, ISO 27001, and a set of technical minimum requirements has been introduced in government that establishes a framework for risk-based management of information security.

There has also been a general strengthening of the skills of citizens and businesses in terms of cyber and information security.

At the same time, there is a strong focus in the EU on enhancing cyber security, including through the revision of the Network and Information Security (NIS) Directive. This also requires Denmark to increase the level of ambition, including in terms of management-based risk control, implementation of security measures and ICT preparedness.

The NIS Directive

The EU Network and Information Security (NIS) Directive

The EU Network and Information Security (NIS) Directive from 2016 is an important instrument in enhancing cyber and information security in the vital societal functions of Denmark. In December 2020, the Commission proposed to revise the Directive to expand the scope. E.g. in the form of new cyber security requirements targeting companies and public authorities and member states' supervision of cyber security. The goal is management-based risk control, implementation of organisational and technical measures, as well as control of emergency preparedness, which enables organisations to handle incidents (before, during and after) and operational cooperation across organisations and national borders in the EU.

Improving cyber security in Denmark requires a concerted effort and a shared responsibility across society. The state is responsible for national security. Companies and public authorities have a responsibility to safeguard the security of their own organisation. Moreover, all citizens need to understand how their actions can affect their own and others' digital security.

The Danish National Strategy for Cyber and Information Security 2022-2024 raises the ambitions and objectives for a cyber and information secure Denmark. The strategy of the Danish government focuses on the security of the critical ICT infrastructure that supports vital societal functions.

Definition of terms

Vital societal functions
The activities, goods and services that are the basis for the general functioning of society.

Critical infrastructure
Infrastructure, including facilities, systems, processes, networks, technologies, assets, and services - necessary to maintain or restore vital societal functions.

Critical ICT infrastructure
The subset of critical infrastructure that includes the digital infrastructure needed to maintain or restore vital societal functions.

ICT systems critical to society
ICT systems where major disruptions result in significant challenges for society as a whole. The unavailability and unstable operation of ICT systems can have significant consequences for society and for the maintenance of processes critical to society.

An ambitious effort targeting government and vital societal functions

Vital societal functions that are robust and resilient require a high level of cyber and information security in the critical ICT infrastructure that support these functions. This requires ambitious efforts from both public and private actors. The strategy is expanded from covering the six current sectors critical to society to include a wider range of ministries with responsibility for IT-supported vital societal functions.

All government agencies must continue to comply with a number of technical minimum requirements, which will be expanded during the strategy period. The same applies to ministries responsible for ICT systems critical to society or vital societal functions for which a number of additional security requirements also apply. Overall, this will contribute to ensuring that ministries with a particular responsibility for vital societal functions is able to act quickly and efficiently in the event of a serious cyber incident.

Cyber and information security in the central government: New requirements for government agencies

Ministries (or parts thereof) responsible for vital societal functions	Must comply with a number of new requirements for organising security work around the vital societal functions, including requirements to set up a DCIS and develop its own cyber and information security strategy for the vital societal functions
Government agencies responsible for ICT systems critical for society	Must comply with a number of new regulatory requirements related to the systems, including new requirements for contract and supplier management, and enhanced requirements for the preparation of contingency plans
All government agencies	Must comply with a set of minimum requirements, including the organisation of security work, compliance with ISO 27001 and technical minimum requirements

Focus on the business sector
Cyber and information security must be a priority for all Danish businesses, especially small and medium-sized enterprises (SMEs). Many SMEs are affected by cyberattacks and the trend is increasing. The approximately 300,000 SMEs must prioritise cyber security, as an attack can have huge costs for the individual company, for example in lost turnover. Ultimately, this can result in a company losing its business foundation and has to cease operations.

With this strategy, the government focuses on a stronger and more coherent effort on SMEs. By strengthening the digital security level of SMEs, we ensure that Denmark remains competitive and has good conditions for growth.

Growth for companies

Growth conditions for the cyber and information security ecosystem in Denmark

A strengthened Danish cyber ecosystem can both create growth in the cyber security industry and boost the general level of cyber security in Denmark across authorities and companies, with a stronger foundation of suppliers who understand the Danish market and its needs. A strong Danish cyber security industry is key to contributing to European strategic autonomy in this area. This requires strong knowledge sharing and networking. The EU has decided to set up national cyber security coordination centres in each Member State to support the cyber security industry and work with the European Cyber security Competence Centre (ECCC).

Citizens
Denmark is one of the countries in the world where the digitisation of the daily life is most advanced. Being able to venture safely in digital daily life requires a high level of trust among citizens in the public ICT systems and solutions.

It can be challenging as a citizen to navigate in a constantly changing threat landscape where new methods of attack and approaches are continuously evolving. Growing cybercrime and digital fraud targeting citizens demand a need for secure digital behaviour and increased knowledge about cyber and information security.

Thus, people in Denmark must be equipped to act in the digital daily life and use digital services and products safely. The strategy aims to raise the level of knowledge and skills of digital behaviour and security among citizens with initiatives that motivate and engage, promote increased knowledge and interest, and develop sound and secure digital habits among citizens.

Hotline

Identity theft hotline

The government has initiated a new hotline for citizens to help with digital identity theft. The hotline was launched in June 2021 by the Danish Agency for Digital Government. The hotline is open 24 hours a day all year round and provides a one-stop shop for citizens who either have been victims of, or suspect, digital identity theft.

Strategic objectives

With the strategy, the government has set four strategic objectives, which sets the framework for the development of a stronger and more secure digital Denmark.

The government wants

1. Robust protection of vital societal functions

- We need to be able to maintain vital societal functions and economic activity in a crisis where critical ICT infrastructure is non-functional for a short or longer period.
- Government agencies and businesses must have a certain level of security to be able to act on a short notice in the event of serious cyber incidents.

2. Increased level of skills and management commitment

- Cyber and information security must be embedded in top management, and skills must be strengthened. This applies to an overview of assets, vulnerabilities and knowledge of potential threats.
- Citizens, businesses and government agencies need to know how to protect themselves and stay safe digitally.
- Demand for cyber and information security skills must be accommodated by training more specialists and building stronger capacity across society.

3. Strengthening of the cooperation between the public and private sector

- Government agencies and businesses need to cooperate more closely and share knowledge and experience about threats and incidents.
- Government agencies and businesses need to be supported with highly specialised consultancy through centralised coordination.

4. Active participation in the international fight against the cyber threat

- International cooperation in the EU, UN, NATO and like-minded countries must be strengthened. It must be difficult and consequential to conduct cyberattacks against Denmark.
- Denmark must actively contribute to ensuring an open, secure and reliable internet, along with protecting critical ICT infrastructure.

1

Robust protection of vital societal functions

- We need to be able to maintain vital societal functions and economic activity in a crisis where critical ICT infrastructure is non-functional for a short or longer period.

- Government agencies and businesses must have a certain level of security to be able to act on a short notice in the event of serious cyber incidents.

Maturity in working with cyber and information security is generally increasing in Denmark, including among government authorities. However, several key challenges remain, including a lack of understanding of the cyber threat in general, and complex ICT systems that makes the work difficult.

Vital societal functions, such as energy supply, rail transport and research, are increasingly digitised, requiring a focus on the critical ICT infrastructure that supports them. There is a need for a better overview of the critical ICT infrastructure and dependencies between the ICT systems that support vital societal functions. Therefore, ministerial areas with responsibility for vital societal functions must have a clear plan for their cyber and information security and be able to participate in operational cooperation and emergency preparedness.

Many government agencies lack basic technical security measures and continue not to comply with the established technical minimum requirements. Likewise, the level of security for a large part of the ICT systems critical to society in the central government is currently inadequate.

Since 2016, government agencies have been required to follow the international security standard ISO 27001, which sets best practices for information security management. Over a third of the agencies have yet to complete the implementation of the standard.

Vital societal functions that are robust and resilient also require that Danish companies have adequate digital security and that the police have the capacity to prevent and investigate cyber-related financial crime.

At present 40% of Danish SMEs have an inadequate level of digital security compared to their risk profile, and many companies lack basic measures in their digital security[1]. As a result, there is a need to strengthen the digital resilience of Danish enterprises, especially SMEs.

Reports of financial cybercrime have increased significantly in recent years. Since its establishment in December 2018, the police's Nationwide Centre for IT-related Economic Crime (LCIK) has received 70,000 reports of financial cybercrime[2]. This underlines the need for enhanced prevention and investigation efforts.

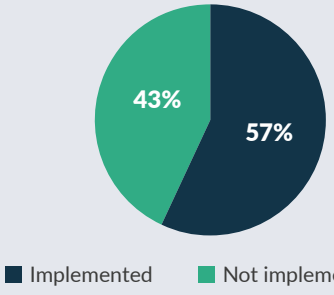
The strategy launches a series of strategic actions to strengthen the security of vital societal functions and ensure that government agencies and businesses have an adequate level of security.

1 Digital security in Danish SMEs 2021

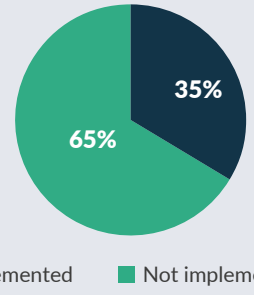
2 Nationwide Centre for Cybercrime

The level of security of government agencies is inadequate in several places

Status of ISO 27001 implementation



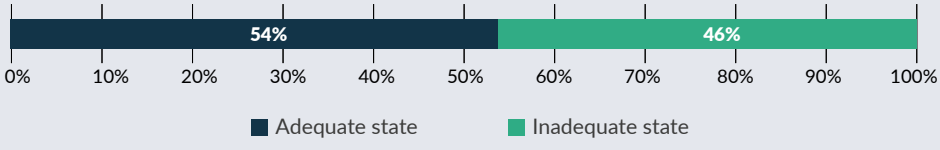
Status of the technical minimum requirements



Government agencies are required to comply with the ISO 27001 security standard and implement 20 technical minimum requirements. Only 57% have fully implemented the ISO 27001, and only 35% comply with all 20 requirements.

Source: Danish Agency for Digital Government

Too many ICT systems critical to society in the central government are in an inadequate state



46% of the ICT systems critical to society in the central government are in an inadequate state. For a large proportion of ICT systems, the cause is the inadequacy of the technical conditions and/or an inadequate level of security.

Source: Danish Agency for Digital Government

Companies have not implemented basic security measures

Security measures deficiencies

24%

of SMEs have not implemented the two basic security measures of back-up and automatic updating of software.

Source: Digital security in Danish SMEs 2021

Inadequate level of security

40%

of SMEs have an inadequate level of digital security in relation to their risk profile.

Source: Digital security in Danish SMEs 2021

Strategic initiatives

- Security and cooperation regarding vital societal functions and ICT systems critical to society will be strengthened with new requirements for the organisation of security work, including requirements for a partial strategy and decentralised cyber and information security units.
- Security requirements for the management of government ICT systems critical to society will be tightened to ensure that security in and around ICT systems has the right managerial focus.
- The security in government agencies will be strengthened by introducing new technical minimum requirements. At the same time, advisory work on the ISO 27001 security standard will be increased to ensure full implementation by all government agencies.
- A stronger technical bulwark will be built within central government with new common technical solutions to protect government employees from phishing and malware. Common government logging is established as an ICT security shield to provide better opportunity to identify and counter threats. The ability of government agencies to report and share threats with each other will also be strengthened.
- A better overview of critical ICT infrastructure supporting vital societal functions will be created.
- Knowledge and awareness of digital security among business managers, employees and advisors, e.g., accountants and bank advisors will be increased. In addition, businesses will have access to powerful and easy-to-use tools that they can use to raise their digital security level, especially targeting the SME segment.
- Police response to cybercrime will be strengthened by expanding the capacity to retrospectively investigate and disrupt as well as enabling the deployment of the police to businesses in the event of a cyberattack.

2

Level of skills and management commitment

- Cyber and information security must be embedded in top management, and skills must be strengthened. This applies in relation to an overview of assets, vulnerabilities and knowledge of potential threats.

- Citizens, businesses and governments need to know how to protect themselves and stay safe digitally, and more specialists with cyber and information security skills need to be trained.

Danes are becoming increasingly aware of cyber and information security[3]. However, there is a challenge in translating awareness into knowledge, skills, and action to boost cyber and information security.

Cyber security requires top management commitment to make security a more integral part of the management function, and this requires the possession of the right skills.

However, SMEs, in particular, lack the skills and resources to implement appropriate security measures. Moreover, there is a cross-cutting challenge in recruiting and retaining relevant cyber and information security skills. The demand for cyber and information security skills is great, but both authorities and companies find it difficult to obtain the right profiles for the tasks. Thus, there is a need to strengthen the supply of skills if security is to be raised across the board.

Finally, there is a need for initiatives to promote increased skills within the Danish population.

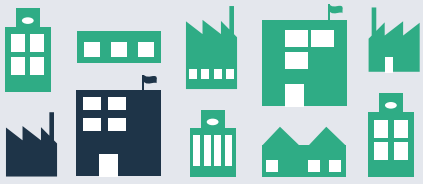
Citizens must be able to act safely in the digital daily life. This applies to children and young people, as well as adults, so that they avoid, to the greatest possible extent, becoming victims of cybercrime or digital fraud.

In order to ensure a high level of cyber and information security across society, the strategy launches several initiatives with a focus on increasing skills and providing a better foundation for top management commitment. Efforts targeting children, young people and adults through education will also be created, to make the Danish population more digitally literate.

> “
>
> The survey *Information Security among Danes 2020* has shown that knowledge about cyber and information security is not sufficiently widespread among the population and among employees in both government agencies and companies

3 Information Security among Danes 2020

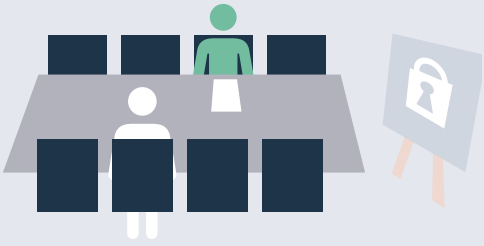
Lack of top management commitment and competencies



22%

of companies and authorities that have tried to recruit information security staff have either been unable to recruit or had to hire a profile that did not have all the desired competencies.

Source: Labour market for information security skills in Denmark

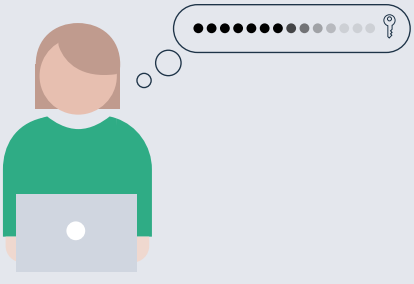


26%

of Danish SMEs make decisions about the company's digital security work, where the management is less than fully involved.

Source: Digital security in Danish SMEs 2021

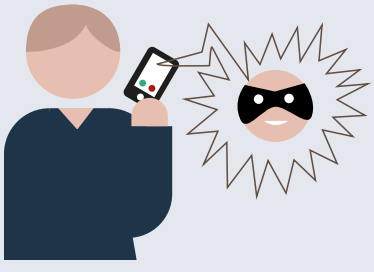
Citizens lack knowledge about cyber and information security



16%

of citizens comply with the recommendation of making a password of more than 12 characters and that this is not reused in multiple places.

Source: Information Security among Danes 2020



21%

of Danes in 2020 received scam phone calls.

Source: Information Security among Danes 2020

Strategic initiatives

- Embedding and prioritising cyber and information security at all levels of management will be ensured by strengthening the knowledge, awareness and behaviour of top managers and leaders in government through increased requirements and expectations as well as new skills initiatives.
- The skills of government employees in cyber and information security will be strengthened with new training initiatives, including the State Digital Academy, which targets both specialists and generalists.
- Equipping children, young people and adults to be digitally literate will be ensured by implementing a broad initiative in the field of education and training, e.g., by disseminating inspirational material and increasing awareness at all levels of education.
- Society's access to cyber and information security skills will be strengthened through higher education, e.g., within ordinary education, and post-graduate and higher education.
- Cyber and information security among citizens, businesses and government agencies will be enhanced by strengthening information efforts aimed at target groups through further development of the information portal, Sikkerdigital.dk.

3

Strengthening cooperation between the public and private sectors

- Government agencies and businesses need to work more closely together and share knowledge and experience about threats and incidents.

- Government agencies and businesses need to be supported with highly specialised consultancy through centralised coordination.

The ability to share knowledge and experiences on cyber and information security incidents is vital to achieve a high cyber and information security level. Therefore, there is a need to strengthen cooperation across sectors so that we can become even better at sharing knowledge and learning from each other. Government agencies also need to be better at using existing data and incident reports to disseminate knowledge about threats and vulnerabilities.

There is a high demand for centralised consultancy, and there is a need to strengthen capacity and the overall advisory support of government agencies to meet this demand.

In addition, citizens and businesses exposed to phishing attempts and hacking are unclear as to where to address their issues and what sort of assistance they need. Citizens can now get advice from the identity theft hotline, but there is a need for broader help and consultancy for both businesses and citizens: this also includes basic cyber and information security.

In the business sector, stronger and closer cooperation is needed. In general, initiatives targeted at SMEs remain fragmented and often only take the form of awareness-raising activities and guidance initiatives. If cyber and information security is to be boosted in the entire business sector, it is crucial that the overall business effort for cyber and information security is coordinated and coherent. Concrete tools are needed to keep Danish companies competitive.

Through a number of concrete actions in the strategy, the government is strengthening public-private cooperation on cyber and information security. The initiatives ensure better opportunities for knowledge and experience exchange, strengthen the advisory efforts towards public authorities, companies and citizens and contribute to the competitiveness of Danish companies through concrete tools.

Unreported figures expected

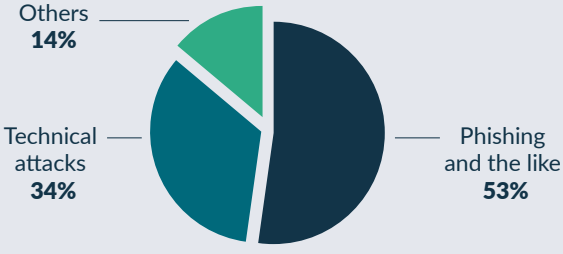
?

Since not all businesses, citizens and authorities are supposed to report all incidents, a significant number of ICT security incidents are expected to go unreported.

Scope of the incident and routes of attack vary

In 2020, the Centre for Cyber Security handled 467 security incidents that had an impact on the affected organisations.

Identified routes of attack 2020



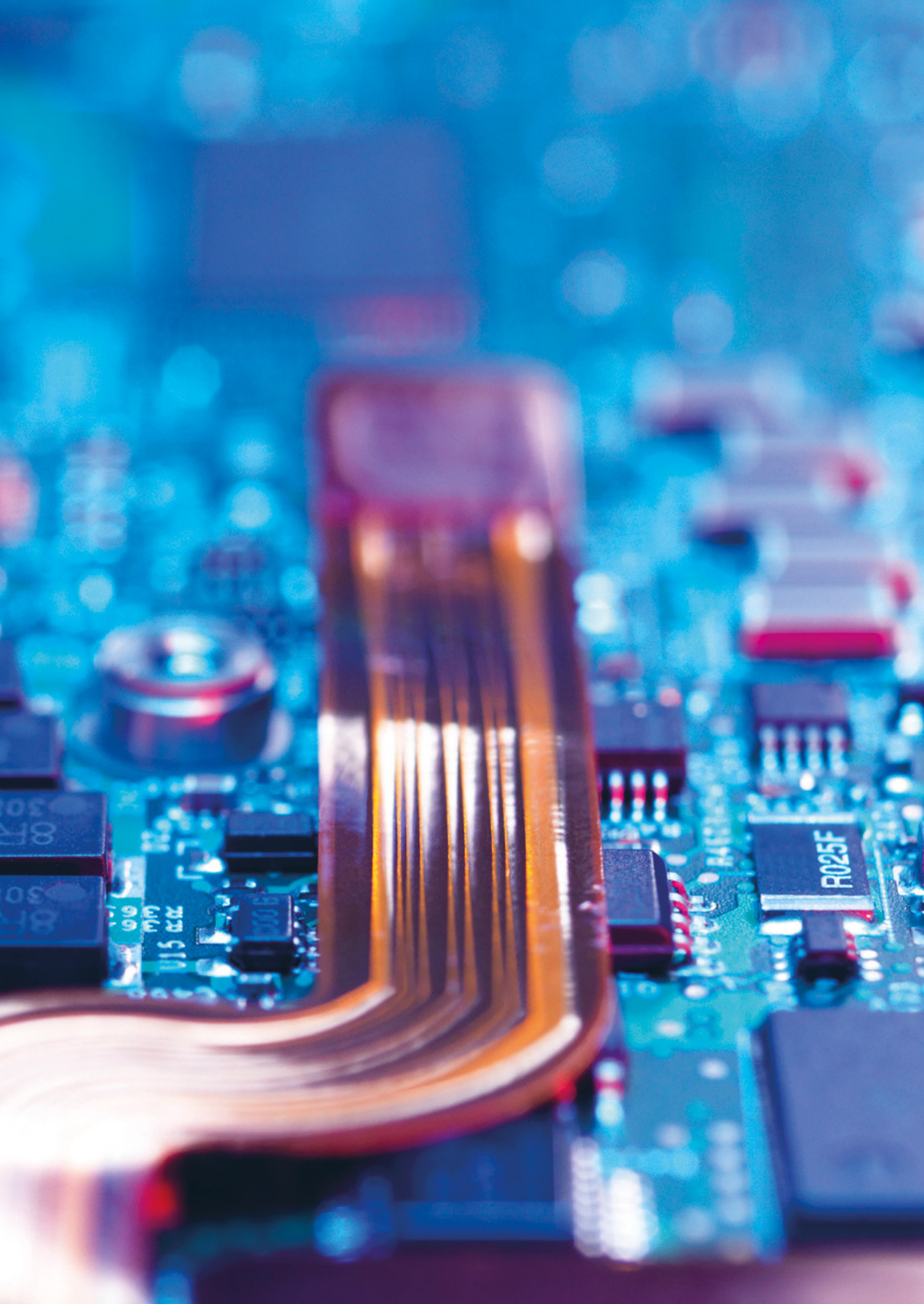
Strategic initiatives

- Better help for citizens and businesses will be offered through a cyber-hotline, where it will be possible to seek advice and guidance if you suspect or have been exposed to cybercrime. The cyber hotline will be combined with the already established identity theft hotline.
- Situation-specific advice to government agencies will be strengthened. The central advisory capacity of the Centre for Cyber Security, which provides advice and guidance on cyber and information security management, will be strengthened.
- Experience sharing and insight into cyber and information security incidents, as well as data sharing between government agencies and businesses, will be strengthened to better provide advice on, warn and prevent incidents.
- Focus on the SME segment will be increased, so that knowledge and experience are intensified. A cyber security unit for SMEs will be established to implement a comprehensive and coordinated effort to strengthen knowledge sharing and cyber security levels at SMEs. Among other things, the unit will help facilitate and launch new public-private initiatives to help strengthen SMEs' cyber security.
- Cooperation and coordination between government agencies on the protection and safeguarding of information across government agencies will be strengthened through advisory services.

Public-private cooperation on cyber and information security

The Danish Cyber Security Council advises the government on how to strengthen digital security and ensure knowledge sharing between authorities, the business sector and the research community. During its first term, the council has contributed to the development of the Danish National Strategy for Cyber and Information Security 2022-2024, held a number of webinars and contributed to the National Cyber Security Month. The Council has also been involved in the development of the SmitteStop app and the digital corona pass.

The Business Forum for Digital Security supports the government's work to promote and strengthen the digital security level of the Danish business sector. The forum contributes to an overall boost to digital security in the Danish business sector, by making recommendations to the government and the business sector and acting as a strategic partner for the government in the development and implementation of concrete initiatives. Including the upcoming cyber security unit for SMEs.


R025F

4

Active participation in the international fight against the cyber threat

- International cooperation in the EU, UN, NATO and with like-minded countries must be strengthened. Conducting cyberattacks against Denmark has to be difficult and have consequences.

- Denmark must actively contribute to ensuring an open, secure and credible internet and protect critical ICT infrastructure.

The digital domain is an integral part of 21st century international politics, and it has become one of the first lines of defence of law-based international order, which too has come under strain.

Denmark is continuously under attack conducted by other states. Malicious actors want to steal valuable information and high-tech knowledge or deploy malware that can later be used in tense situations. Although Denmark can do much on its own, there is a need for strengthening international cooperation within the organisations that can develop norms and define standards for cyberspace if the underlying causes of cyberattacks are to be fought.

Certain authoritarian states are actively trying to undermine the application of international law in cyberspace and increase control over the internet, while at the same time exploiting the same global ICT infrastructure for cyberattacks, influence campaigns and aggressive cyber espionage. When a rule-based international order does not exist in cyberspace, the distinction between war and peace becomes blurry. This makes it difficult for Denmark and our allies to deter and to respond to malicious cyber activity. In addition, it compromises our safety, security and economic progress. There is therefore a need to be able to hold criminal actors accountable and be able to deter and counter malicious cyberattacks.

Multinational cyber security companies are often the first to detect and respond to cyberattacks. In addition, tech and cyber security companies are, therefore, vital partners when it comes to developing and maintaining stability, order and rules in cyberspace. Thus, there is a need to improve cooperation between governments and private companies at the strategic and political level, and to clarify the division of responsibilities and tasks when dealing with specific cyber incidents.

In order to face the challenges, but also to take advantage of the opportunities that exist on the international cyber and information security scene, the strategy initiates a number of efforts in order to strengthen Denmark's international profile, build stronger bridges to the international tech and cyber security industry and ensure that it remains expensive and costly to conduct cyberattacks and espionage against Denmark and our allies.

Strong focus on cyber security in the EU with the following initiatives

- Establishment of a cyber diplomacy toolbox, which forms the basis for the EU to increasingly call attention to the cyber threat, and through which sanctions have been adopted against hackers from Russia, China and North Korea.
- The decision to establish the European Cyber security Competence Centre (ECCC) and the Network of National Coordination Centres, which will, among other things, enhance the competitiveness and resilience of the European cyber security industry and turn cyber security into a competitive advantage for EU companies.
- A revision of the NIS Directive, putting additional focus on cyber security in critical sectors and among suppliers to these sectors.
- A revision of directives, inter alia, the directive for products and radio equipment, in order to include cyber security.
- Prioritising cyber security in the European funding programmes, Digital Europe and Horizon Europe, including the establishment of cross-border cooperation between industry, research institutions and government agencies.
- Launch of an EU cyber security strategy, including focus on building collective resilience in Europe.

European framework for cyber security certification

Increased digitisation of everything from toothbrushes to cars, increased use of the internet and storage of data and systems in the cloud means increased risk of cyberattacks. It is a risk that is difficult for both citizens and businesses to understand and to protect themselves against adequately. To strengthen cyber security and the internal digital market, the EU has adopted regulation that allow for the cyber security certification of products, services and processes. This will make it easier for citizens and businesses to be better informed about which products and services that meet the relevant safety requirements.

Strategic initiatives

- Denmark's efforts in international cooperation for an open, secure and reliable internet will be strengthened through an increased involvement in the EU, NATO and the UN.
- Denmark's position and profile when it comes to international cyber cooperation will be boosted, with the aim of strengthening the possibility of diplomatic responses, including sanctions and work for active defence using offensive cyber capacity.
- The deterrence of cyberattacks will be strengthened by raising the costs of attacking Denmark, our allies or our close partners in cyberspace by strengthening Denmark's contribution to detecting, deterring and prosecuting individuals, actors and organisations that abuse digital networks to steal and spy on the people in Denmark, companies and government agencies.
- Export control of digital products from Danish companies and help to businesses to effectively freeze the financial assets of criminals will be improved and strengthened.
- Cooperation with the multinational tech industry, think tanks and academia to counter cyberattacks and other hybrid threats will be strengthened through technological diplomacy and the direct channel to tech company headquarters.

Governance

- Responsibilities and roles for authorities' work on cyber and information security

The cyber and information security work is organized according to the principle of sectoral responsibility. This means that the authority, which has day-to-day responsibility is also responsible in the event of a serious incident. This applies with respect to daily preparedness, during an ongoing incident and in connection with recovery work following an incident.

Intra-sector incidents
The entity (authorities, businesses and organisations) which has day-to-day responsibility for a given service or function will continue to have this responsibility in the event of a cyber incident. In connection with this, the entity must ensure that it receives assistance from any operational supplier. Furthermore, the entity may request assistance from decentralised cyber security units. The entity is responsible for requesting this assistance and for preliminary incident management.

Furthermore, depending on the scope of the incident, the entity is responsible for reporting the incident to all competent authorities and to the Centre for Cyber Security. Finally, the entity is responsible for any external communication concerning the incident.

Major cross-sectoral incidents
In connection with major cyber incidents that affect several sectors, The National Operative Staff (NOST, which includes among its permanent members the Danish National Police, the Danish Security and Intelligence Service and the Danish Defence Intelligence Service/the Centre for Cyber Security) may be activated.

Principle of sectoral responsi-bility

Among other things, the principle of sectoral responsibility implies that:

1. All ministers must ensure an appropriate emergency response within their own remit.
2. Sector-specific responsibility encompasses all critical functions and services required by law, politically or administratively.
3. The authorities' emergency response planning must be based on an ongoing and systematic risk assessment process, for which management assumes overall responsibility.
4. The public authorities must monitor the risk scenario for their own sector on a regular basis.

However, in these situations the principle of sectoral responsibility continues to apply, which means that it is the authorities responsible for the relevant sectors who must ensure that a comprehensive overview of the scope of the incident is carried out and the reporting of this to the relevant authorities, including to the Centre for Cyber Security (and to the National Operative Staff if this unit has been established), just as it is the responsibility of the affected authorities, businesses and organisations to manage the incident and its consequences. Depending on the scope and nature of the incident, the Centre for Cyber Security may assist the entities affected by the incident in their response. For instance, the Centre for Cyber Security may carry out technical investigations of cyberattacks with a view to stopping the specific incident, as well as to clarify any methods of attack or vulnerabilities, such that prevention of similar situations can be improved. These investigations will be carried out in close collaboration with the entity that has been subject to the incident.

In connection with the majority of major cyberattacks there will be a need for both general investigations and technical, ICT-security investigations. To this end, close cooperation has been established between the police (including the Danish Security and Intelligence Service) and the Centre for Cyber Security. This cooperation entails mutual briefing in the event of major cyber incidents, including intentional attacks. Similarly, concerted operational efforts will typically be implemented in connection with specific incidents.

Communication

As a general rule, external communication in connection with minor incidents which do not affect several sectors will be managed by the authority responsible for the relevant sector. Communication concerning cyber threats and the current situation report as well as other crisis communication in connection with cyber incidents is the responsibility of the Centre for Cyber Security in collaboration with the authority responsible for the relevant sector.

Communication will need to be coordinated in the event of a major, cross-sectoral incident. This coordination is the responsibility of the Central Operational Communication Staff (DCOK) under the auspices of National Operative Staff (NOST). The DCOK is responsible for ensuring rapid disclosure and coordination of relevant information to the general public, including to the media. The DCOK is also tasked with establishing ad hoc units from which the public can obtain further information concerning the specific incidents.

Government bodies with cross-sectoral responsibility for cyber and information security

Public authorities' work with cyber security will be supported through assistance, information, guidance and advice from government bodies with cross-sectoral and coordinating functions in the field. Public authorities must actively request the assistance they require.

Government bodies that supply information, advice and guidance on cyber and information security matters

1. The Centre for Cyber Security is the national authority on ICT security. The centre is responsible for a number of tasks of a preventive and mitigating nature, including advisory services. The Centre for Cyber Security's infrastructure and Internet security service can help detect and warn of advanced cyberattacks on authorities and businesses that subscribe to the service. The Centre for Cyber Security warns relevant authorities and businesses about specific cyber threats. The centre also prepares national and sector-specific situation reports and threat assessments.

2. The police are tasked with preventing and investigating IT-related crime and with stopping such crime. The police also have a coordinating role in the event of major, cross-sectoral incidents.

3. The Danish Security and Intelligence Service is the national security authority for Denmark and provides consultancy and assistance to public authorities and private businesses in security matters, including the handling and storage of documents based on the safety circular.

4. The Danish Agency for Digital Government supports information security in the public sector, including through guidance on ISO 27001 and setting requirements for government agencies, including as part of the government's ICT portfolio management. In addition, the Danish Agency for Digital Government carries out a number of citizen-focused information tasks, including Sikkerdigital.dk and the identity theft hotline. The agency is also responsible for coordinating the implementation of the strategy in concert with the Ministry of Defence.

5. The Danish Business Authority is tasked with developing and offering knowledge, guidelines and tools and coordinating efforts aimed at strengthening digital security in the wider business community, especially in SMEs.

Appendix

Initiatives

Robust protection of vital societal functions

1.1 Strengthened security regarding vital societal functions
1.2 Critical ICT systems in the central government need to be more secure
1.3 Better security through ISO implementation and new minimum requirements targeting government agencies
1.4 Greater focus on ICT security in public ICT procurement and tendering
1.5 Common technical solutions
1.6 Strengthening digital resilience and digital management commitment in SMEs
1.7 Strengthening police efforts against cybercrime
1.8 Increased web patrolling
1.9 Recovery of data and critical ICT systems in the central government
1.10 Legal basis to counter broad and disruptive destructive cyberattacks
1.11 Expanded analysis of critical national ICT infrastructure
1.12 Coordinated vulnerability Disclosure (CVD) within central government
1.13 Strengthened accreditation and technical security audits
1.14 Focus on ISPs' ability to block malicious domains
1.15 Alternative to satellite-based time management
1.16 Strengthening the first-time registration of foreign nationals in the Central Population Register

Increased level of competence and management commitment

2.1 Strengthened efforts in relation to knowledge, awareness and conduct for top management and government leaders
2.2 Government employees need better skills in cyber and information Security
2.3 Competencies in cyber security for children, young people and adults
2.4 Competence building in cyber and information security through higher education
2.5 Knowledge sharing and cyber and information security in in the field of research and education
2.6 Strengthened information efforts for citizens, authorities and businesses and strengthening of the portal, Sikkerdigital.dk

Strengthening cooperation between the public and private sectors

3.1 Better help for citizens and businesses through a cyber-hotline

3.2 Strengthened central advisory capacity

3.3 Establishing a cyber security unit for SMEs

3.4 Strengthened exchange of experiences and insights into cyber and information security incidents

3.5 Enhanced investigative capability for cyber espionage

3.6 Strengthening the protection of the information of the central government

3.7 Strengthened security oversight of system vendors and data processors

Active participation in the international fight against cyber threats

4.1 Strengthening the contribution to a rules-based international order

4.2 Diplomatic responses

4.3 Strengthened capacity to counter cyberattacks by state and non-state actors

4.4 Strengthened deterrence of cyberattacks

4.5 Strengthening controls on the proliferation of cyber products and the freezing of economic resources

Robust protection of vital societal functions

1.1 Strengthening security around vital societal functions
Ministerial areas responsible for vital societal functions that are significantly IT-enabled are required to develop cyber and information security strategies and establish a decentralised cyber and information security unit (DCIS). The strategies will initially cover state-owned critical ICT infrastructure and in the next phase address the private, regional and municipal sectors.

1.2 Critical ICT systems in the central government need to be more secure
New cyber and information security requirements are introduced for government agencies responsible for ICT systems critical to society. Since a significant part of the government's ICT systems critical to society are currently outsourced to private suppliers, the possibility for the government to take over the ICT systems, if necessary, must also be considered if the supplier in question goes bankrupt or decides to liquidate its business.

1.3 Better security through ISO implementation and new minimum requirements for government agencies
The management of information security in the central government is strengthened by increasing guidance initiatives in relation to ISO 27001. At the same time, security is strengthened through the further development of minimum technical requirements, which are mandatory for all government agencies.

1.4 Greater focus on ICT security in public ICT procurement
In order to improve cyber and information security among public authorities, it needs to be identified how ICT security aspects can be better integrated into public framework and procurement contracts, and whether the level of ICT security in the contracts is sufficiently transparent for the authorities.

1.5 Common technical solutions
Several common solutions are being established to strengthen security among the authorities, including 1) a joint state-safe DNS service to protect government employees against phishing and malware, 2) a joint state security shield (GovShield), which, through logging and the possibility of expansion, must help identify and counter cyber threats against authorities that are not customers of the central government's IT, 3) an effective reporting system for phishing emails (phishing portal), so that sharing information about threats and indicators of compromises is improved. In addition, 4) a National ICT Contingency Plan will be established, which authorities will have to take into account in their contingency plans.

1.6 Strengthening digital resilience and digital management commitment in SMEs
The digital resilience of Danish SMEs is increased by giving their management, employees and existing advisors the best possible conditions to secure themselves against the digital threat with, among other things, a user-friendly and interactive toolbox and a bridge-building effort.

1.7 Strengthening police efforts against cybercrime
Strengthen police response to cybercrime by expanding the capacity to investigate and disrupt cybercrime from behind the scenes and enable police to deploy to businesses in the event of a cyberattack.

1.8 Increased web patrolling
Under the multi-year agreement for the police and the prosecution, a web patrol unit will be set up in the Danish police, which will enable the police to prevent, monitor and investigate activities in the digital space in order to prevent cybercrime.

1.9 Recovery of data and ICT systems critical to society in the central government
Government agencies must have plans in place to be able to recover data and ICT systems critical to society in the event of damaging incidents. Guidelines and instructions must be developed for the application of recovery plans and tests in the central government, with a view to more government agencies testing their recovery plans. In addition, the efforts of the Centre for Cyber Security are strengthened regarding assistance with recovery, particularly in cases of importance to national security.

1.10 Legal basis to counter broad and disruptive destructive cyberattacks
The feasibility of building the capability to counter disruptive or destructive cyberattacks against vital societal functions in Denmark by providing the legal basis to take down compromised servers will be examined.

1.11 Expanded analysis of critical national ICT infrastructure
An analysis of the digital dependencies between critical ICT infrastructures is to be carried out. The analysis will be a supplement to the ongoing mapping of critical infrastructure in Denmark. The purpose is to equip society to continue vital societal functions in a better way if these are affected by major or global cyber security incidents.

1.12 Government CVD policy

A pilot of a government CVD (Coordinated Vulnerability Disclosure) policy will be launched. A government CVD policy will describe the framework for government agencies to allow private individuals ("helpful hackers") to identify and report vulnerabilities in ICT systems.

1.13 Strengthened accreditation and technical security audits

The capacity of the Centre for Cyber Security to accredit ICT systems that process classified information is strengthened. In addition, the capacity to conduct technical safety inspections, to a limited extent, for special authorities is strengthened, as well as guidelines and advice from authorities in this regard.

1.14 Focus on ISPs' ability to block malicious domains

The possibility for ISPs to provide DNS blocking of malicious domains as a standard service will be explored. The aim is to strengthen the ability to identify, remove or block malicious domains and thereby achieve greater security for Internet users in Denmark.

1.15 Alternative to satellite-based time management

A cross-sectoral analysis is to be prepared of the need to establish one or more time management systems as an alternative to the existing satellite-based time management system. The aim is to create a framework for the establishment of robust and accurate time management, on which many current and future technologies in Denmark depend.

1.16 Strengthening the first-time registration of foreign nationals in the Central Population Register

Training efforts will be launched for control staff of relevant authorities to ensure more valid personal data in the Central Population Register, which is a prerequisite for trust in the personal data used by many public and private bodies.

Increased level of competence and management commitment

2.1 Strengthened efforts in relation to knowledge, awareness and conduct for top management and government leaders
Increased demands are placed on the personal ICT security of top government leaders, and competence initiatives are strengthened so that security will become a integral part of the management task in the future.

2.2 Government employees eed better skillswithin the field of cyber and information security
New competence initiatives will be launched to ensure that all government employees know what constitutes safe digital conduct and can put it into practice.

2.3 Competencies in cyber security for children, young people and adults
New initiatives are being launched in primary schools to strengthen the management of data in the education sector through guidelines and awareness-raising activities. This will ensure that children, young people and adults are equipped to navigate safely in a digital world.

2.4 Competence building in cyber and information security through higher education
New training elements in mainstream education and a strengthened effort in higher education and follow-up training will contribute to reducing the skills gap in cyber and information security in society.

2.5 Knowledge sharing and cyber and information security in the field of research and education
Increased focus is being placed on cyber security in the educational offer in the research and educational environments.

2.6 Strengthened information efforts for citizens, authorities and businesses and strengthening of the portal Sikkerdigital.dk
Sikkerdigital.dk will become Denmark's common and authoritative information portal for help and guidelines on digital security. This is to ensure a high level of knowledge and competence among citizens, authorities and companies, including large companies. By building on the information efforts, the conduct of each target group also needs to be addressed.

Strengthening cooperation between the public and private sectors

3.1 Better help for citizens and businesses through a cyber-hotline
A government hotline will be established for citizens and businesses, including large enterprises, to seek help and guidance on basic cyber and information security. The hotline should also be able to provide concrete guidelines on, for example, data recovery, phishing attempts and/or securing data for possible subsequent police investigation. The hotline is established in close cooperation with Sikkerdigital.dk.

3.2 Strengthened central advisory capacity
The initiative strengthens the central advisory services of the Centre for Cyber Security in a number of areas: (1) strengthening the highly specialised advisory unit with a focus on situational advice to government agencies with regard to solution-specific and practical challenges; (2) increasing the capacity to conduct security technological studies; (3) strengthening the analytical capacity in relation to cybercrime and cyber espionage; and (4) strengthening the capacity of the telecommunications section with regard to being able to follow the development of 5G technology and provide advisory service.

3.3 Establishing a cyber security unit for SMEs
In order to have a comprehensive and coherent initiative targeting SMEs, a cyber security unit will be established to, among other things, gather and share SME-relevant knowledge and experience on incidents and threats. Among other things, the unit will help facilitate and launch new public-private initiatives to help strengthen SMEs' cyber security. The initiative is adapted to different types of SMEs, as they have varying levels of maturity and needs.

3.4 Strengthened exchange of experience and insight into cyber and information security incidents
Possibilities must be investigated for strengthening the exchange of experience and knowledge building across public and private actors and between sectors, so that relevant knowledge about specific incidents is shared as widely as possible. There is also a need to look at how data from, for example, the Danish Data Protection Agency and the Danish National Police can be made more available to others.

3.5 Enhanced investigative capability for cyber espionage
The Danish Security and Intelligence Service's capacity to investigate cyber espionage by state actors is strengthened.

3.6 Strengthening the protection of the information of the central government
A national coordination group is set up to strengthen cooperation and coordination between authorities and to step up advisory efforts in relation to the physical security at government agencies.

3.7 Strengthened security oversight of system vendors and data processors
A cost-effective basic model for the supervisory task is being developed with a view to strengthening and streamlining the authorities' supervision of data processors and system suppliers in the field of information security and data protection. Based on the results, a concept test of the supervision model can be carried out on one or more ICT systems in the central government.

Active participation in the international fight against cyber threats

4.1 Strengthening the contribution to a rules-based international order
Through significantly strengthened efforts in the UN and other norm and standard-setting organisations, as well as through increased cooperation with the tech industry, Denmark will increase its contribution to a rules-based international order in cyberspace and shape the rules of the game in an area that is crucial for our security, safety and economic prosperity.

4.2 Diplomatic responses
Denmark's capacity to initiate and engage in international coordination of diplomatic responses to cyberattacks, such as attributions and sanctions, is strengthened, including in the EU context, with a view to increasing Denmark's deterrence profile in the cyber area.

4.3 Strengthened capacity to counter cyberattacks by state and non-state actors
A number of actions are being implemented to strengthening national cyber defence, including 1) strengthening the Cyber Analysis Division of the Centre for Cyber Security to increase technical attribution capabilities, 2) it must be possible to track influencing activities abroad on social media, 3) establishing an offensive cyber defence capable of detecting preparations by, warning of, deterring and countering cyberattacks by state and non-state actors against Denmark or our allies, 4) the Danish knowledge building and influence in the field of cyber operations and security in NATO is strengthened through the secondment of staff and 5) strengthening cyber security at the embassy level through the recruitment of designated technical standards, technical solutions and the institutionalisation of sustained dedicated cooperation in this area.

4.4 Strengthened deterrence of cyberattacks
An active cyber defence must be built that will enable us to disrupt, mislead or stop an adversary's cyber operations against Denmark. This includes the deployment of a liaison officer to Europol's Joint Cyber Action Task force (J-CAT).

4.5 Strengthening controls on the proliferation of cyber products and the freezing of economic resources
Controls on the proliferation of cyber products are being strengthened so that Denmark does not proliferate sensitive technology that cybercriminals can access. At the same time, we need to help businesses become better at freezing criminals' funds for use in cyberattacks.

December 2021

The Danish Ministry of Finance
Christiansborg Slotsplads 1
1218 Copenhagen K
Denmark
Tel: +45 3392 3333
E-mail: fm@fm.dk

ISBN 978-87-93073-51-7 (digital version)
ISBN 978-87-93073-52-4 (printed version)

Design: BGRAPHIC
Photos: Getty Images

The publication can be downloaded
at fm.dk / regeringen.dk

The Danish Ministry of Finance
Christiansborg Slotsplads 1
1218 Copenhagen K
Denmark
Tel. +45 3392 3333
E-mail: fm@fm.dk