THE DANISH GOVERNMENT

Danish Cyber and Information Security Strategy

Ministry of Finance

MAY 2018

Content

Preface

In common with the rest of the world, technological development in Denmark is currently accelerating. Moreover, Denmark is increasingly connected via digital solutions, and public authorities, businesses and citizens are becoming ever more dependent on the Internet and on the opportunities afforded by the Internet.

Denmark is one of the most digital countries in the world, and digital solutions are key to the development of the public sector and for the growth and competitiveness of private businesses.

Citizens are used to interacting with businesses and public authorities via digital solutions and have a basic trust that exchange of data and information takes place in a responsible and secure manner which respects the privacy of the individual.

Confidence in the security of digital solutions is crucial for the continued digital development of the Danish society. There is a need to protect our data and ensure that the digital solutions on which our welfare society depends are protected against damaging external attacks.

The government is now increasing its cyber and information security efforts and will invest DKK 1.5 billion in cyber and information security over the next few years.

With the 2018-2023 Defence Agreement the government and the parties responsible for the agreement significantly reinforced measures to protect Denmark against cyber threats. This work is now being further consolidated by a new national cyber and information security strategy that ties together the various efforts.

The government will launch 25 initiatives and six targeted strategies addressing the most critical sectors' cyber and information security efforts to enhance the technological resilience of digital infrastructure, improve citizens', businesses' and authorities' knowledge and skills and strengthen coordination and cooperation in this area. The strategy will consolidate cyber and information security in Denmark and ensure systematic and coordinated action over the coming four years.

The threat of malicious cyberattacks cannot be eliminated. However, by means of a new cyber and information security strategy, the government will ensure that society can continue to benefit from technological opportunities, and that citizens can retain confidence in digital development.

/The Danish government

Digital Opportunities and Vulnerabilities

Denmark is one of the most digitised countries in the world. This is true both of the public sector, where the majority of tasks and communication with citizens have become digital, and of private businesses, which make extensive use of digital opportunities for creating growth and new business models. It is likewise true of the Danish population as a whole, which is among the most digital-ready populations in the world. The high degree of digital solutions offers great benefits and a range of new perspectives for citizens, businesses and society as a whole. Among other things, it attracts foreign investment and helps ensure that society remains competitive.

Over the coming years, the digital transformation of both public and private sectors will continue. The development of new technologies will accelerate, and the range of digital solutions will continue to grow. Public authorities will make continuous use of digital solutions to provide better and more efficient and effective services for citizens, and businesses will utilise these solutions to generate growth and increase employment.

However, the digital transformation of society also brings with it an increasing dependency on digital solutions, with an associated vulnerability to incidents that lead to ICT system breakdowns or breaches of confidentiality, accessibility and integrity of data. Such incidents may be the result of attacks or by an individual's unintentional breach of information security. Public authorities and businesses have a fundamental responsibility to ensure that security is aligned with the challenges which digital development also presents.

In its national cyber and information security strategy, together with a series of sub-strategies targeting the most critical sectors in society, the Danish government has set out an ambitious plan for the coming years' work of ensuring that Denmark is digitally secure. In the coming years, the Danish central government together with sectors that are of vital importance to society, such as the energy,

“

Authorities and businesses have a fundamental responsibility to ensure that security is aligned with the challenges

Information security
Information security is a broad term for the overall measures to secure information with regard to confidentiality, integrity (changing of data) and accessibility. Data security encompasses organisation of security measures, impact on behaviour, data processing procedures, supplier management and technological security measures.

Cyber security
Cyber security encompasses protection against breaches of security resulting from attacks on data or systems via a connection to an external network or system. Cyber security thus focuses on vulnerabilities inherent to the interconnection of systems, including connections to the Internet.

transport, telecommunications, finance, healthcare and maritime sectors must increase their efforts to ensure the necessary level of cyber and information security throughout Denmark. This work must build on the national efforts of recent years which have helped increase the level of cyber and information security, but the government now intends to accelerate this process. Threats are developing at a rapid pace, and this necessitates a significant strengthening of efforts such that these challenges are met.

Increased dependency and increasing vulnerability

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. At the same time, citizens, businesses and authorities are increasingly the target of ever more sophisticated attempts by malicious third parties to steal and exploit data.

As systems and infrastructures become increasingly integrated, and when several devices are connected to the Internet, the associated security challenges become more complex. What at first may appear to be an isolated and relatively minor security incident can quickly spread across authorities, businesses and sectors.

Moreover, many public authorities face the challenge of large and complex, and in some cases outdated, ICT system portfolios, making it difficult and expensive to maintain the requisite level of security. Furthermore, much of the critical ICT infrastructure in a number of sectors such as the financial, transport and health sectors, is supported by private businesses. To these may be added the many small and medium-sized businesses which are the backbone of the Danish business structure. If private businesses do not have in place an adequate level of security, they may become the target of attack, breaches, data leaks, and contribute to the spreading of incidents to the rest of society.

As such, ensuring society's resilience and security has become a more complex challenge. As a society, we must not only protect ourselves against various types of attack, but also against system breakdown, supplier failure, intentional and unintentional breaches of cyber and information security and the compromising of personal data.

“As systems and infrastructures become increasingly integrated, the associated security challenges become more complex

Inadequate security culture
Lack of security skills and lack of knowledge present a significant vulnerability which may be exploited by malicious third parties. The security behaviour of the managers and employees of authorities and businesses is vital to achieving an adequate level of protection.

High dependency on digital infrastructure
Vital digital infrastructure is a precondition for carrying out activities in the public and private sectors. Lack of accessibility, integrity and confidentiality in digital infrastructure can have significant repercussions for society.

More connected devices
An increasing number of devices are connected via the Internet. This provides new opportunities, but also increases vulnerability to attacks due to the potential for more rapid spread of security incidents.

High level of complexity in the IT portfolio
Many public and private organisations are dependent on complex, and often outdated, ICT systems. Frequently the software used by these systems is not adequately maintained and the systems often do not have the requisite level of security.

Cyberattacks can be carried out cheaply and easily
The ready availability of hacking tools on the Internet means that anyone who wish to hack a system can do so relatively easily and cheaply.

An evolving threat scenario

In recent years, digital development has provided state-sponsored groups, foreign states, activists and criminals with new methods to carry out cyber-related attacks against countries, businesses and citizens. This is a global challenge faced by all open and digital societies which is expected to increase in coming years.

Cyberattacks can take many forms and comprise incidents in which third parties attempt to disrupt or gain unauthorised access to data, systems, digital networks or digital services. Examples of this are attacks on public authority or business websites, or more sophisticated attacks in the form of attempts to gain access to confidential information and data from businesses and public organisations – or even attempts to cause breakdown or disruption.

Cyber and information security threats affect all areas of society. The consequences for victims range from loss of small amounts of money to loss of information and data vital to one's business. Such attacks can have repercussions for central government security and lead to loss of central government integrity, significant material or financial loss and, in extreme cases, loss of life. For the Danish government, it is essential that Denmark continuously adapts its efforts in this area to address the changing threat scenario.

Cyber and information security threats affect all areas of society

The strategic foundation: National Strategy for Cyber and Information Security 2015-2016

The objective of Denmark's first national cyber and information security strategy for 2015-2016 was to enhance the Danish government's cyber and information security efforts as well as to raise awareness of cyber and information security among citizens and businesses. The strategy included requirements for implementation of the ISO27001 international security standard and requirements for systematic and professional monitoring of information security in central government.

The strategy contained several initiatives aimed at raising awareness of cyber and information security among citizens, businesses and authorities. The Centre for Cyber Security established a threat assessment unit and an advisory centre for ICT security. In addition, the Agency for Digitisation launched campaigns aimed at the entire population in the strategy period. The Danish police's investigative capacity with respect to information security was increased, and guidance on information security was consolidated. Finally, the Danish Business Authority developed a digital security check for small and medium-sized businesses in particular, and a business advisory board on ICT security (Virksomhedsrådet for It-sikkerhed) was set up in order to promote sustained dialogue on strengthening the information security framework for businesses. In March 2017 the board submitted its recommendations on how to strengthen ICT security and encourage responsible handling of data particularly in small and medium-sized businesses.

The strategy also identified a need to improve the dialogue between educational institutions and employers which hire graduates from these institutions. On this basis, a collaboration was established, anchored in three innovation networks with strong competencies within cyber security in research and the business community. Among other things this collaboration has resulted in the development of a new professional undergraduate programme in ICT security.

A Systematic and Sustained Effort

The government's vision for cyber and information security efforts in Denmark

- Citizens, businesses and authorities must be familiar with and be able to manage digital risks, such that Denmark can continue to use digital solutions to support the development of the society.

The increasing social and economic role of digital solutions places completely new demands on information security, and the negative consequences of not having a structured approach to security can be profound. At the present time, there is a need for systematic and coordinated efforts, and for this reason the Danish government is now intensifying its focus on this area.

Danish society must be able to function in a secure and responsible manner. This requires that our digital infrastructure is resilient to cyber threats, and that citizens, businesses and authorities continuously improve their digital skills. This applies to security specialists, who will be in even greater demand over the next few years. It also applies to private individuals whose knowledge of how to navigate safely in a digital world will have to be continuously improved so as to support a high level of information security in Denmark.

A joint responsibility

Improving the level of national cyber and information security is a joint responsibility. The central government is responsible for safeguarding national security. Businesses and authorities are responsible for safeguarding security at their own organisations. Moreover, all citizens will have to understand how their actions can affect their own digital security and that of others.

With the Danish Cyber and Information Security Strategy 2018-2021 the Danish government is taking the next step towards a more secure digital Denmark. The strategy focuses on three areas: technological preparedness; raised awareness of cyber and information security among citizens, businesses and authorities; improved cooperation and coordination between responsible authorities. Moreover, sub-strategies for cyber and information security in the most critical sectors will ensure that the individual sectors take action where it is most needed.

Private enterprises own and subsidise much of the infrastructure in sectors responsible for functions that are vital to society. As such there is a need for close cooperation between the public sector and the private sector as well as between civil society, the police and the Armed Forces. The initiatives set out in the strategy focus in particular on cyber and information security within the sectors of energy, transport, telecommunications, finance, healthcare and the maritime sector as well as within central government organisations.

The Danish government will launch 25 specific initiatives to bolster cyber and information security in Denmark. Some of these initiatives build upon efforts that have already been launched, while others are entirely new. The strategy also serves to forge links between a number of cross-cutting activities taking place in the authorities responsible for cyber and information security in Denmark.

Part of a broader initiative

The Danish Cyber and Information Security Strategy is part of a broader initiative. The government has placed a great emphasis on cyber security, and via the 2018-2023 Defence Agreement, Denmark's cyber defences will be considerably reinforced through an injection of DKK 1.4 billion over six years. This will include better protection against sophisticated cyber-attacks by expanding the Centre for Cyber Security's sensor network for authorities and businesses. Moreover, a national cyber situation centre will be established. This centre, which will be manned day and night, will provide an overview of the national security situation with current and potential threats to Denmark's most essential digital networks. The Centre for Cyber Security, which is a national ICT security authority, will also significantly strengthen its capacity to advise and support private businesses and public authorities.

The EU Directive on Security of Network and Information Systems (the NIS Directive)

Denmark is currently transposing the EU Directive on Security of Network and Information Systems (the NIS Directive). One of the requirements set out in the directive is that operators of services that are essential for maintaining key societal functions and services must take steps to manage the security of networks and information systems used to provide their services. A further requirement set out in the directive is that member states must draw up a national strategy for the security of network and information systems. This is something the Danish Cyber and Information Security Strategy takes into account.

The EU General Data Protection Regulation

The new EU General Data Protection Regulation will enter into force on 25 May 2018. The regulation will be complemented by a new data protection act which enters into force simultaneously and will provide additional protection of personal data in Denmark.

As part of a consolidated concerted effort on the part of central government authorities, the work of the Danish Defence Intelligence Service will be strengthened with respect to impact operations. Among other things, the analytical capacity of the Danish Defence Intelligence Service will be expanded. Finally, the Danish Armed Forces' capacity to carry out military cyber operations will continue to be expanded.

The signatories to the Defence Agreement have earmarked a portion of the agreement funds for the purpose of tackling future cyber challenges through additional initiatives, including research and training. This will ensure that Denmark is able to address future challenges.

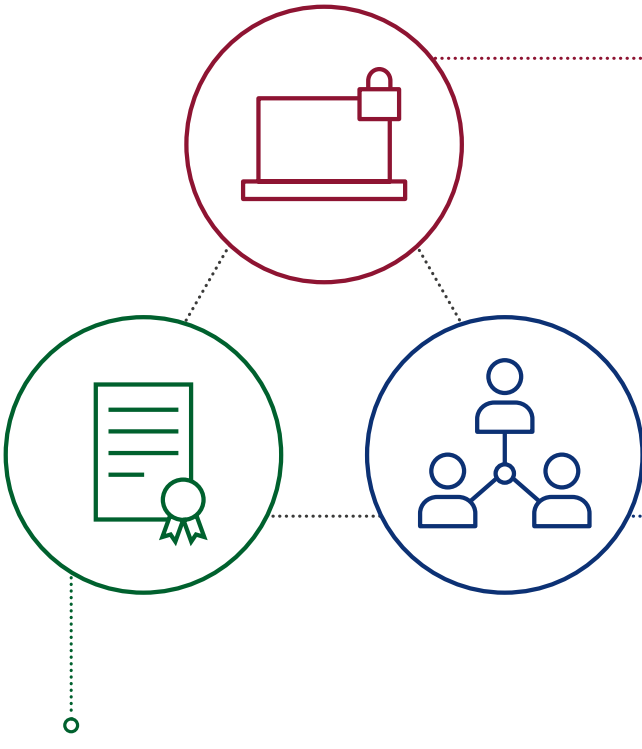
In its capacity as a national security authority, the Danish Security and Intelligence Service is also planning to intensify its cooperation with relevant authorities and private businesses in order to help Denmark address security threats in the best possible manner.

Finally, in January 2018, the government presented its Strategy for Denmark's digital growth, which aims to ensure that Denmark becomes a digital frontrunner. The strategy contains a number of initiatives aimed at improving businesses' ICT security and responsible handling of data in order to ensure digital confidence in the use of new technological possibilities.

In parallel with this, as part of the common public sector Digital Strategy for 2016-2020, it has been agreed that municipal and regional information security efforts must be further consolidated. The government will enter into a dialogue with municipalities and regions concerning further initiatives in this area based on the Danish Cyber and Information Security Strategy.

Benchmarks

The Danish government has defined three clear benchmarks for becoming stronger and more digitally secure as a country over the coming four years.



Everyday Safety for Citizens and Businesses
Central government together with critical sectors is enhancing its technological preparedness as the threat scenario evolves in order to be able to protect essential societal functions against cyberattacks or other major information security incidents.

Better Competencies
Citizens, businesses and authorities have access to the requisite knowledge and are qualified to address the increasing level of cyber and information security challenges.

Joint Efforts
Risk-based security management is an integral part of central government management and management of critical sectors. There must be a clear division of roles and responsibilities in the area of cyber and information security for authorities and businesses providing key societal functions.

Initiatives

Everyday Safety

1.1 Creating a national cyber situation centre
1.2 Minimum requirements for authorities' work on cyber and information security
1.3 Regulatory initiatives in the cyber area
1.4 Monitoring of critical ICT systems in central government
1.5 Common digital portal for reporting
1.6 National centre for processing of cases concerning ICT crime
1.7 Enhanced collaboration on prevention of ICT-related attacks and enforcement in response to such attacks
1.8 Higher security for identity documents
1.9 Improved prioritisation of national ICT infrastructure
1.10 Secure communication in central government

Better Competencies

2.1 Digital judgment and digital competencies acquired via the educational system
2.2 Information portal
2.3 Research into new technology
2.4 Corporate partnership to increase ICT security in the Danish business community
2.5 Collaboration on competence development and the fostering of a security culture in central government
2.6 Improved awareness drives aimed at citizens and businesses

Joint Efforts

3.1 Sub-strategies at sectoral level and decentralised cyber security units
3.2 Cross-sectoral efforts to support cyber and information security in critical sectors
3.3 Management of suppliers of outsourced ICT services
3.4 Strengthened national coordination
3.5 Increased level of involvement in international collaboration
3.6 Evaluation of the current state of cyber and information security
3.7 Overview of information worthy of protection
3.8 Information security architecture
3.9 National and international efforts to safeguard data ethics and protection of personal data

Everyday Safety

Initiatives

1.1 Creating a national cyber situation centre

1.2 Minimum requirements for authorities' work on cyber and information security

1.3 Regulatory initiatives in the cyber area

1.4 Monitoring of critical ICT systems in central government

1.5 Common digital portal for reporting

1.6 National centre for processing of cases concerning ICT crime

1.7 Enhanced collaboration on prevention of ICT-related attacks and enforcement in response to such attacks

1.8 Higher security for identity documents

1.9 Improved prioritisation of national ICT infrastructure

1.10 Secure communication in central government

Everyday Safety for Citizens and Businesses

Benchmark: Central government and the critical sectors are enhancing their technological preparedness as the threat scenario evolves in order to be able to protect essential societal functions against cyberattacks or other major information security incidents.

In order to safeguard the operation of essential societal functions and protect vital ICT systems and data, the Danish government will:

- Establish a better overview of threats and strengthen the monitoring of systems and data that are vital to society.
- Increase the cyber and information security level of government authorities.
- Enhance national advisory efforts.

The Danish government wishes to consolidate Denmark's resilience to cyberattacks. Awareness of threats, identification of vulnerabilities and assessment of risks constitute important factors in this context. Individual businesses and authorities are responsible for handling their own cyber and information security and for adapting their efforts on the basis of risk assessments and vulnerability analyses. Each organisation is responsible for ensuring implementation of necessary security measures and for sufficient protection of ICT systems and data.

This demands awareness and an overview of potential threats. As such, Denmark's ability to identify and manage Internet-based threats to the Danish state and critical sectors needs to be expanded and strengthened.

Improved overview and enhanced monitoring

In order to protect ICT systems and data of critical importance to society, it is crucial that the central authorities have a complete overview of the specific systems and data that require protection, and that monitoring of vital systems and data is carried out. This monitoring must allow for notification of the authorities and businesses concerning potential and current threats, and must support authorities and businesses in protecting themselves and being capable of maintaining vital societal functions.

In order to guarantee ongoing monitoring, the government will establish a national cyber situation centre at the Centre for Cyber Security. This cyber situation centre, which will be manned day and night, will provide a continuously updated overview of the national security situation, identifying current and potential threats to Denmark's most important digital networks, and this will contribute to the authorities' comprehensive overview in the national crisis management system.

The authorities, together with certain types of businesses, are required to report cyber incidents to the relevant public authorities. Reports submitted by the authorities and by businesses are a prerequisite for the necessary knowledge-sharing and aggregation of experience, and for maintaining an updated overview of the number of ICT security incidents, types of incidents and their repercussions. In order to facilitate reporting the Danish government will establish a single digital solution for the reporting of ICT security incidents. This solution must also have the ability to send back to the reporter action-oriented information concerning the prevention and handling of incidents. A single digital solution will on the one hand support businesses and authorities in reporting as many relevant security incidents as possible, and on the other help to provide more nuanced and detailed insight into the ICT security incidents affecting Danish businesses and the Danish authorities.

Increased state effort on cyber and information security

Since 2016, the Danish government authorities have had an obligation to comply with the requirements of the international security standard ISO27001, which sets out best practice for information security management. The most recent follow-up on the government authorities' implementation of the ISO27001 indicates that work remains to be done before the standard has been fully implemented. For instance, the authorities must become better at carrying out risk assessments and ongoing evaluation of their efforts. With this strategy, the government is sharpening its focus on ensuring a high minimum level of ICT security for all government authorities.

In the future, all government authorities will be subject to minimum requirements for work on cyber and information security. These minimum requirements will concern both technical and organisational aspects, and will support a consistent approach to the work and ensure a sufficiently high level of protection against cyber and information security incidents. This will entail the government authorities improving their work on risk-based information security management through ISO 27001, preparing action plans for managing and developing the ICT portfolio (including management of legacy challenges and information security), actively reaching a documented decision on instruction products in the area, and implementing tried and tested technology to protect against attacks.

In order to ensure comprehensive implementation of ISO 27001 within central government organisations, the Danish government will in the future follow up on the organisations' implementation efforts once every six months. The government will request that authorities who have yet to implement the standard submit an action plan to the government describing what measures they plan to implement in order to ensure comprehensive implementation of the standard.

Enhanced national advisory efforts

The Centre for Cyber Security is a national ICT security authority responsible for preventive national advisory and information activities associated with cyber security in both the public and the private sector, as well as a targeted effort to address specific incidents.

The 2018-2023 Defence Agreements, will considerably reinforce the centre's preventive efforts through enhanced advisory and guidance efforts aimed particularly at critical sectors.

At the same time, the centre's capacity to identify specific incidents will be reinforced. In combination with the centre's advisory services, this increased capacity will support the work of the authorities and businesses responsible for restoring security following a cyberattack in critical sectors.

Risk-based approach

The authorities' and businesses' work on information security must be based on a risk assessment. This includes an assessment of the commercial and financial risks associated with maintaining the business objectives in the event of potential security incidents, including cyberattacks, and what constitutes appropriate security measures in order to reduce the risk to an acceptable level.

This assessment presupposes an overview of the organisation's systems, including their technical design and vulnerabilities. Based on the prioritisation determined on the basis of the risk assessment, appropriate measures will be launched to counter the identified vulnerabilities.

Initiatives – Everyday Safety

Initiative 1.1: Creating a national cyber situation centre

A national cyber situation centre will be created at the Centre for Cyber Security. The cyber situation centre will be manned day and night and will provide a national overview of the current state of security for digital networks which serve a crucial societal function. The situation centre will carry out technical monitoring of networks and scan intelligence sources, media and forums for information concerning new threats and ongoing potentially serious cyberattacks. Furthermore, the centre will function as a national contact point for cross-border cyber security incidents.

Initiative 1.2: Minimum requirements for authorities' work on cyber and information security

An appropriate level of minimum requirements for handling cyber and information security within government authorities must be secured. All government authorities must adhere to the principles set out in the ISO27001 information security standard and assess the need for certification. Authorities which have not fully implemented the standard must submit an action plan to the government that sets a direction for ensuring full implementation of the standard. Furthermore, the authorities must actively reach a documented decision on their use of instructions on cyber and information security, assess the need to implement tried and tested technologies to protect against malicious cyber and information security incidents and meet the requirements set out in the Strategy for ICT management in central government.

Initiative 1.3: Regulatory initiatives in the cyber area

The rapid pace of change to the threat scenario entails a need to adapt legislation to address the current threat scenario as well as technological developments, such that the Centre for Cyber Security will be better prepared to respond to cyberattacks against critical infrastructure. The Danish Ministry of Defence will accordingly present a proposal to amend legislation in the cyber area, thereby giving the Centre for Cyber Security a better scope for identifying and preventing cyberattacks while simultaneously enhancing the Centre's analytical work.

Initiative 1.4: Monitoring of critical ICT systems in central government

As a result of changes to the threat scenario there is a need to expand proactive monitoring efforts to safeguard critical ICT systems in central government. Accordingly, a monitoring centre will be established at the Agency for Governmental ICT Services, which will be manned day and night. This initiative will provide all customers at the Agency for Governmental ICT Services with the possibility for 24-hour monitoring of systems operated by Agency for Governmental ICT Services. The initiative will be phased in gradually, and the monitoring centre will be fully functional by 2020. Authorities whose systems are not operated by the Agency for Governmental ICT Services must take steps to ensure 24/7 monitoring if, on the basis of a risk assessment, this is deemed necessary.

Initiative1.5: Common digital portal for reporting

Reporting security incidents must be a simple and easy matter for businesses and authorities alike. For this reason a shared digital solution for reporting security incidents will be established. The solution must help ensure that businesses only have to report an incident once and in one location. Furthermore, the solution must enable the communication of action-oriented information concerning prevention and handling of incidents back to the reporter. The digital portal for reporting of security incidents will be accessible via Virk.dk, which already serves as the digital portal for businesses and authorities reporting to the public authorities.

Initiative 1.6: National centre for processing of cases concerning ICT crime

In order to ensure a consistent and consolidated effort to combat ICT crime, a national centre will be established under the auspices of the Danish police to handle the receipt and preliminary processing of reports of ICT crime. The centre will support the police in taking a more data-driven approach to their work on combating and preventing crime.

Initiative 1.7: Enhanced collaboration on prevention of ICT crime and enforcement in response to such crime

IT-related attacks can be carried out at a great distance between the perpetrator and the victim, and by means of technological solutions that may challenge the tried and tested methods of fighting such attacks. Therefore, it is important that the relevant authorities possess the tools and capacities required to effectively prevent attacks from happening or escalating. The existing collaboration between authorities with shared responsibility in the area must continuously secure the best possible basis for fighting ICT-related attacks at all times. To this end, a working group will be established with participants from the Ministry of Defence and the Ministry of Justice.

Initiative 1.8: Higher security for identity documents

As a society, we must be able to have confidence in the identities and identity documents created and issued by public authorities. This applies to both physical and digital identity documents such as passports, driver's licences and *NemID* ("Easy ID" – the national digital signature solution). To this end, efforts will be launched to ensure cohesion between registration of a physical identity document and issuance of a digital identity document, as well as to ensure cohesion across various systems in the public sector.

Initiative 1.9: Greater prioritisation of national ICT infrastructure

A comprehensive list will be drawn up of authorities and businesses with digital infrastructure which provide functions that are of vital importance to society. A description will be given of the key businesses and authorities, together with any services, of particular importance to cyber and information security efforts in Denmark. The description, in combination with a threat assessment, will form the basis for greater prioritisation of the Centre for Cyber Security's monitoring activities and the countering of cyberattacks by authorities and businesses responsible for the sector, as well as for the ongoing work on cyber and information security in a broader sense.

Initiative 1.10: Secure communication in central government

There is a need for broader access to secure communication between authorities. Accordingly, it will be made easier for government authorities to use networks with a high level of security to communicate with each other, and a solution for secure communication by mobile telephone will likewise be provided.

2

Better Competencies

Initiatives

2.1 Digital judgment and digital competencies acquired via the educational system

2.2 Information portal

2.3 Research into new technology

2.4 Corporate partnership to increase ICT security in the Danish business community

2.5 Collaboration on competence development and the fostering of a security culture in central government

2.6 Improved awareness drives aimed at citizens and businesses

Better Competencies

Benchmark: Citizens, businesses and authorities have access to the requisite knowledge, and possess the necessary prerequisites to handle the increasing level of cyber and information security challenges.

In order to support the improvement of competencies among citizens, businesses and authorities, the Danish government will:

- Improve digital judgment and digital skills among children and young people.
- Raise awareness of cyber and information security among citizens, businesses and public authorities.
- Support continuous enhancement of specialist knowledge and expertise in the area.
- Support cyber and information security efforts in the business community.

Increased digitisation and the constantly changing threat scenario place greater demands on the digital security awareness and digital skills of private individuals, businesses and organisations when it comes to addressing cyber and information security threats.

The rapid development of new technologies and criminals' ability to exploit these technologies constantly presents new challenges. For this reason, it is necessary to raise awareness among citizens of cyber and information security issues, and to ensure that the digital behaviour of citizens and businesses becomes more secure.

Digital judgment and digital competencies acquired via the educational system

Many young people lack sufficient knowledge about how to protect themselves and others on the Internet, or about which third parties they need be wary of. In this context, the educational system plays an important role in ensuring that all children and young people are equipped to navigate in a safe, responsible and ethical manner when using ICT technology and social media.

Accordingly, the Danish government will focus on digital skills in a security perspective starting in primary and lower secondary school, and continuing through to graduation. Children and young people should be offered the best opportunities to embrace digital possibilities and adopt a critical approach as members of a digital society. Children and young people must have the ability to think critically about content on the Internet such that they are wary of the threat presented by fake news, radicalisation, cyberbullying, online fraud, etc. They should be in a position to safely navigate the Internet and to exploit digital opportunities in a safe and secure manner. Moreover, they must be aware of the rules and consequences associated with being online. Children and young people should be taught to be digitally competent, develop strong critical faculties with respect to digital matters and understand the attendant ethical dilemmas in addition to the necessary technological skills associated with digitalisation.

“

Children and young people must have the ability to exploit digital opportunities in a safe and secure manner

Raised awareness of cyber and information security

All citizens, authorities and businesses need to be aware of cyber threats. Moreover, they must continuously improve their knowledge of such threats and of how to tackle them in a safe manner. They also need to be aware of the risks to which they expose themselves and others.

To this end, the government will establish an information platform aimed at citizens, businesses and authorities. Citizens, businesses and public authorities need to be able to locate relevant, specific and useful information and tools which will enable them to protect themselves in the best possible way. Information efforts will help increase awareness of threats, while the information portal will promote a higher level of knowledge that enables people to take the necessary precautions.

As technological development progresses, the challenge of maintaining government authorities' cyber and information security becomes more complex, and the requisite competencies will become increasingly in demand both among specialists and generalists. At the same time, the private sector is experiencing an increasing demand for skilled labour. The government will therefore invite all relevant parties to participate in a partnership on competency development in the area.

To improve competencies in central government the Danish government will also launch a number of initiatives aimed at central government managers, employees and specialists, such that they can continue to

develop and digitise the government sector towards the necessary level of security. A number of the courses held by the digital academy, which was presented by the government in autumn 2017 as part of the Strategy for ICT Management in Central Government, will therefore focus on safe online behaviour and on cyber and information security.

Knowledge concerning new technologies

Alongside the need for more knowledge there is a need for more security specialists to support secure digital conversion of businesses and public authorities. These specialist skills are vital in a digital age, and are crucial to ensure Denmark's ability to maintain cyber and information security.

Through more targeted research into the importance of new technology in tackling digital vulnerabilities, the Danish government will generate more knowledge surrounding the best possible measures, models and tools for achieving cyber and information security. This will be made possible by strategic research funds for research into new technological opportunities.

Research in this area will also provide more certified training in cyber security at educational institutions, and thereby support the aim of ensuring that the workforce of the future has the necessary skills and expertise demanded by businesses.

Strengthened cyber and information security efforts in the business community

The government will support a general consolidation of cyber and information security in the business community. In common with the rest of Denmark, businesses have embraced digital transformation. Workflows have been automated, paper archives and account books have been digitised and entered into ICT systems, and sales and marketing activities are increasingly carried

out via the Internet. This promotes growth and renders businesses more competitive, but dependency on digital systems also increases these businesses' vulnerability to cyberattacks.

Danish businesses are increasingly falling victim to cyberattacks. A cyberattack can have serious consequences for the individual business, but attacks, breaches and data leaks in large number of small and medium-sized businesses are also a potential route via which incidents can spread.

The government will now focus on strengthening cyber and information security in the business community. This task will be carried out collaboratively together with business community stakeholders, and a partnership will be established focusing on greater ICT security and responsible handling of data in the business community.

This partnership will form the framework for a joint effort to promote ICT security and responsible handling of data and to disseminate joint solutions to cross-sectoral issues. The partnership will develop preventive security measures and launch efforts to promote businesses' use of international security standards. Finally, the partnership will focus on how to implement efforts to increase insight into ICT security on the part of primary advisors in businesses, such that these advisors are in a position to promote ICT security at Danish small and medium-sized businesses.

With its Strategy for Denmark's digital growth, the government also decided to maintain the business advisory board on ICT security (Virksomhedsrådet for It-sikkerhed), which will make regular recommendations to the government and the business community on strengthening the framework for businesses' ICT security and responsible handling of data. The board will have a role as the advisory board for the partnership, and will be able to make recommendations and provide input on specific business-oriented solutions.

Technology pact

At present there is a serious lack of employees with digital and technological skills at Danish businesses. As advanced technology and digital solutions become more widespread, businesses' are experiencing a growing demand for engineers, computer scientists, biostatisticians, electricians and other personnel with digital and technological skills. For this reason, the Danish government has initiated a technology pact to increase the number of young people who take an interest in the digital and technological field and wish to train and work within this field.

With the technology pact the government has set a goal of ensuring that 20% more young people complete a vocational or higher education programme over the coming ten years within the STEM disciplines (technology, ICT, natural sciences and mathematics).

Source: Strategy for Denmark's Digital Growth, April 2018.

Initiatives – Better Competencies

Initiative 2.1:
Digital judgment and digital competencies acquired via the educational system

Joint efforts will be launched throughout the educational system, focusing on raising awareness of security challenges for children, young people and teachers. Continuing and further education and training programmes will be developed, as well as teaching material and awareness drives on cyber and information security aimed at teachers, pupils and students.

Initiative 2.2:
Information portal

An information portal will be established which will contain readily accessible information and advice, specific tools for citizens, businesses and authorities regarding information security and data protection, as well as information on how to comply with current legislation. The content of the portal will be dynamic, current and regularly updated with the most recent knowledge.

Initiative 2.3: Research into new technology

The Danish government will earmark more funds for technological research, including funds for the RESEARCH2025-team (FORSK2025) project: "New technological possibilities" within the auspices of Innovation Fund Denmark. These research efforts will focus on generating knowledge about new models and tools to assess threats, knowledge to bolster the infrastructure against attacks as well as knowledge that can help improve the ability of authorities and businesses to identify attackers.

Initiative 2.4: Corporate partnership to increase ICT security in the Danish business community

The Danish government wishes to improve ICT security and responsible handling of data in the Danish business community, and to help ICT security become one of Denmark's strengths. In order to achieve this, it will be necessary to work together across the public and private sectors. Moreover, this requires close dialogue and exchange of knowledge between the various players, who each in their way can support businesses' work on ICT security and responsible handling of data. Accordingly, the Danish government will take the initiative to establish cooperation between the public sector and the private sector via a corporate partnership on increased ICT security and responsible handling of data. The business advisory board on ICT security (Virksomhedsrådet for It-sikkerhed) will continue and serve as the advisory board for the corporate partnership.

Initiative 2.5: Partnership on competency development and creation of a security culture in central government

Competencies relating to cyber and information security will become increasingly in demand both among specialists and generalists. The Danish government will therefore invite all relevant parties to participate in a partnership on competence development in this area. In addition, a number of initiatives will be launched to develop the competencies of government employees. Employees need to be equipped to continue the development and digital transformation of the government sector towards the required level of security.

Initiative 2.6: Expanded awareness drive aimed at citizens and businesses

There is a need to expand awareness drives aimed at citizens and businesses to reinforce safe behaviour on the Internet and raise awareness of this matter on a regular basis. National awareness drives will be launched, supplemented by targeted efforts aimed at groups of citizens and businesses who face particular challenges when it comes to digital communication, together with local efforts aimed at businesses or specific groups of employees in the public sector. Private and public stakeholders will be invited to participate as contributors and partners in these efforts.

3

Joint Efforts

Initiatives

3.1 Sub-strategies at sectoral level and decentralised cyber security units

3.2 Cross-sectoral efforts to support cyber and information security in critical sectors

3.3 Management of suppliers of outsourced ICT services

3.4 Strengthened national coordination

3.5 Increased level of involvement in international collaboration

3.6 Evaluation of the current state of cyber and information security

3.7 Overview of information worthy of protection

3.8 Information security architecture

3.9 National and international efforts to safeguard data ethics and protection of personal data

Joint Efforts

Benchmark: Risk-based security management is an integral part of central government management and management in critical sectors. The division of roles and responsibilities in the area of cyber and information security is clearly defined for authorities and businesses which provide functions that are of vital importance to society.

In order to guarantee joint efforts in cyber and information security, the Danish government will:

- Launch initiatives to support work on cyber and information security in critical sectors.
- Place greater demands on authorities' management of suppliers of IT systems that are of vital importance to society.
- Strengthen strategic coordination at national level.
- Increase Denmark's level of involvement in international collaboration in this area.

Cyber and information security tasks are carried out by a range of different authorities, each serving different roles. The ongoing digital transformation and associated growing digital dependency within society raise the need for increased coordination between authorities in this area. This requires a higher degree of central, strategic integration of efforts and initiatives at the national level.

The nature of security challenges means that today cyber and information security must be a key focus for all managers – both in the public and the private sector. At the same time, cyber and information security in Denmark not only depends on central government efforts but also on efforts in sectors of vital importance to society. For this reason, it is necessary to support cyber and information security efforts in central government, in the individual sectors and in relation to citizens and the general business community through increased exchange of experience and coordination. This will help increase Denmark's level of security and utilise a focus on cyber and information security as a strategic opportunity for achieving greater growth and

prosperity, rather than simply viewing it as an operational challenge.

Strengthened efforts in critical sectors

In order to maintain cyber and information security in Denmark, it is crucial that sectors which are of vital importance to society focus on this area. The government will therefore launch initiatives to improve cyber and information security efforts in critical sectors.

Varying levels of maturity and needs in the individual sectors mean that efforts must be tailored to suit the requirements of the various sectors. Dedicated cyber and information security units will be established to help assess threats at sectoral level, strengthen monitoring, establish security systems and develop competencies, and advise and guide authorities and businesses operating within these sectors.

Sector-specific strategies

Sectors of particular importance to cyber and information security in Denmark must have a clear plan for what cyber and information security efforts they intend to implement in their respective sectors. As such, these sectors must prepare sector-specific strategies that are based on the particular conditions which apply for the sector in question. When preparing these sub-strategies, the sectors must involve relevant stakeholders in their work.

Energy

A secure energy supply is a precondition for a well-functioning society. Therefore, lack of security in the energy sector constitutes a vulnerability for society as a whole. The energy sector's vulnerability to cyber threats is growing rapidly as the scale of digitisation increases, encompassing everything from wind turbines to household appliances.

> The cyber and information security in Denmark depends also on efforts in sectors of vital importance to society

In the future, suppliers of digital equipment, software or monitoring will play a more important role in the supply of energy. Furthermore, there is now a greater dependency on digital control of installations for exchange of energy with neighbouring countries and for regulating fluctuations in energy production from solar and wind energy. For this reason, rules have been established concerning contingency plans in the electricity and natural gas sectors, including specific ICT contingencies, such that new threats, vulnerabilities and risks can be identified and managed at an early stage. The energy sector sub-strategy must build upon the work already undertaken within the existing framework.

The Danish Ministry of Energy, Utilities and Climate is responsible for preparing a sub-strategy for cyber and information security in the energy sector, to be completed by the end of 2018 at the latest.

Healthcare

The healthcare sector is characterised by registration of a large amount of personal information relevant to treatment and care in connection with medical-record keeping, documentation requirements and reporting to registers, and by the use of digital and medical devices, etc. This contributes to making the healthcare sector a potential target for cybercrime, with third parties hacking into systems and accessing personal data. The extensive cooperation on patient treatment in the healthcare sector, combined with the sharing of patient data between the stakeholders involved, also entails a risk that potential cyber criminals will attack "the weakest link" unless all stakeholders comply sufficiently with the necessary and uniform security requirements. On this basis, the sub-strategy aims to strengthen and align work on cyber and information security across the healthcare sector in order to predict, prevent, identify and tackle cyberattacks, and in order to continue the work of the Digital Health Strategy 2018-2022, in which a cyber-political forum prioritises cyber security in all areas of the healthcare sector.

The Ministry of Health is responsible for preparing a sub-strategy for cyber and information security in the healthcare sector, to be completed by the end of 2018 at the latest.

Transport

Critical infrastructure in the transport sector is increasingly supported by ICT systems, enabling centralised monitoring and remote or automated control. As the scale of digitisation increases, so too does the threat of attacks targeted at functions and systems that are critical to ensuring a transport sector with a high degree of mobility and secure traffic flows. The sub-strategy for cyber and information security will cover the entire transport sector. However, the areas with the greatest dependency on network and information systems are aviation, and to some extent the railways. Therefore these areas are particularly vulnerable to threats to cyber and information security. The sub-strategy will provide an overview of the challenges faced by the transport sector due to increased use of electronic control systems and automated data exchange. As such the sub-strategy will form the basis for the overall prioritisation of work

on cyber and information security in the transport sector, focusing partly on ensuring maintenance of transport functions that are of critical importance to society, and partly on passenger safety.

The Ministry of Transport, Building, and Housing is responsible for preparing a sub-strategy for cyber and information security in the transport sector, to be completed by the end of 2018 at the latest.

Telecommunication

A central characteristic of the telecommunications sector is that the telecommunications network is one of the most critical elements of our society's ICT infrastructure. Accordingly, when drafting the Act on Security of Network and Information Systems, the Danish government placed a focus on ensuring that telecommunications providers maintain a high degree of information security. As one element of this, telecommunications providers must ensure accessibility, integrity and confidentiality in their telecommunications networks, and must have in place a contingency plan that ensures maintenance of societal functions to the greatest possible extent in the event that the telecommunications network is affected by accidents, natural disasters or cyberattacks.

The Ministry of Defence is responsible for preparing a sub-strategy for cyber and information security in the telecommunications sector, to be completed by the end of 2018 at the latest.

The financial sector

In the financial sector a sectoral forum has been set up, the Financial Sector Forum for Operational Robustness (FSOR). One of the aims of this forum is to ensure a joint, coordinated effort on cyber and information security. Furthermore, the NIS Directive will be transposed in Danish financial legislation by May 2018. The sub-strategy will complement the transposition of the NIS Directive and further develop

the work of the existing FSOR by implementing specific initiatives. Based on the sector's vulnerabilities and current maturity, these initiatives will contribute to greater resilience to cyberattacks and thus to improved cyber security in the financial sector.

The Ministry of Industry, Business and Financial Affairs is responsible for preparing a sub-strategy for cyber and information security in the financial sector, to be completed by the end of 2018 at the latest.

Maritime sector

Sectoral responsibility in the maritime sector covers security related to navigation in Danish waters as well as security of ships registered under the Danish flag, together with their crew. Cyber security for ships includes services such as traffic monitoring, warnings and navigation information (AIS, NAVTEX), systems used by ships and software for operation of the ship, including propulsion and navigation. The sub-strategy will complement the implementation of the NIS Directive by implementing specific initiatives. Based on the sector's vulnerabilities and current maturity, these initiatives will contribute to greater resilience to cyberattacks and thus to improved cyber security in the maritime sector.

The Ministry of Industry, Business and Financial Affairs is responsible for preparing a sub-strategy for cyber and information security in the maritime sector, to be completed by the end of 2018 at the latest.

Drinking water supply

No separate sub-strategy will be prepared for the drinking water supply sector, on the basis that the supply of drinking water is not dependent on network and information systems, given that all utility companies can be manually operated. However, municipal authorities are obliged to have a contingency plan in place that safeguards the supply of drinking water.

It cannot be ruled out that, over time, changes to the utility companies' operations will lead to greater dependency on ICT control of the drinking water supply. The Ministry of Environment and Food will regularly assess whether a sub-strategy needs to be developed for the drinking water supply sector.

Cyber-security package

The European Commission has proposed a comprehensive cyber-security package, of which the overall aim is to achieve resilience, deterrence and defence to protect Europe against cyber threats, while at the same increasing European citizens' confidence in digital solutions. The cyber-security package continues the progress made with the EU Cybersecurity Strategy of 2013, in which the Network and Information Security Directive (NIS directive) was a key element. The European Commission's cyber-security package contains a wide range of initiatives, including a proposed regulation to strengthen the mandate of the EU Cybersecurity Agency (ENISA), as well as a common European framework for cyber-security certification.

Domain name systems (DNS) and digital services

The NIS Directive imposes requirements on DNS providers and administrators of top domain names as well as providers of certain digital services, including cloud computing services, to manage risks associated with the security of their services and to report significant security incidents. These requirements will be implemented via the Ministry of Industry, Business and Financial Affairs' new Act on Security of Network and Information Systems in relation to domain name systems and certain digital services.

Management of suppliers of critical ICT services

A major portion of Danish authorities' critical ICT systems is operated by private providers. This places great demands on government authorities to ensure that their providers maintain an appropriate level of security, that information and data are treated in accordance with legislation, and that citizens' rights with respect to their personal data are respected.

Accordingly, the government will introduce stricter requirements for all public authorities concerning adequate security and control provisions in future contracts for critical ICT systems, and for government authorities' management of private-sector suppliers. Finally, the government will explore the possibility of authorising central government to take over key ICT systems operated on behalf of a government authority in the event that this is deemed necessary under exceptional circumstances.

More co-operation and improved national coordination

The principle of sectoral responsibility implies that the authority responsible for a given function on a day-to-day basis is also the responsible authority when a serious incident occurs. This responsibility also includes planning how to maintain and continue to supply functions in the event of an extraordinary incident. Consequently, responsibility for cyber and information security, and thus the task of protecting our critical infrastructure, is divided between the authorities responsible for the critical sectors, i.e. the transport sector, the healthcare sector and the financial sector. The 2018-2023 Defence Agreement will significantly enhance the ability of the Centre for Cyber Security to assist central government authorities responsible for the various sectors.

The division of responsibilities between the sectors ensures that the initiatives take account of the characteristics and maturity of the individual sector with regard to cyber and information security. Furthermore, sectoral responsibility necessitates central coordination, both between the relevant ministries and between authorities who share this responsibility. It is crucial that central government lays down the overall strategic framework for cyber and information security and supports work in this area in the critical sectors. To support and assist the individual sectors in their work of ensuring adequate cyber and information security a temporary task force will be set up, comprising participants from the Agency for Digitisation, the Centre for Cyber Security and the Danish Security and Intelligence Service.

In order to accommodate the need to swiftly adapt cyber and information security efforts to the ongoing changes of the threat landscape, it is necessary to strengthen national cross-sectoral coordination in this area. For this reason, the government will set up a national steering committee on cyber and information security. A higher degree of coordination and knowledge--sharing in the area will improve cohesion between operational initiatives in the individual sectors and the overall strategic approach to cyber and information security.

Furthermore, the government intends to continue its collaboration with experts from the public and the private sector, and as a consequence of this the Forum for Dialogue on Information Security (Dialogforum for informationssikkerhed) will be reorganised into an advisory board of experts whose role will be to provide input to the implementation and follow-up on the cyber strategy and its initiatives.

Increased level of involvement in international collaboration

In the coming years, the cyber area will be a matter of top priority within the EU, and the European Commission has among other things proposed a comprehensive cyber package. Cyber security will attain a significance which cuts across a number of sectors and areas, including industrial policy, energy security and security of supply, telecommunications, defence, law as well as digitisation in the public and private sector. Accordingly, the government wishes to stregthen Denmark's level of involvement in international collaboration. The ambition is for Denmark to be better represented in discussions at EU, NATO and UN level, where these discussions concern cyber security and control of the Internet and when they directly affect Danish citizens, businesses and public authorities.

The government also wishes to bring the Danish tech-ambassador into play in the cyber area in order to further strengthen the dialogue with large, multinational tech companies and the tech industry in general on cyber and information security, including data ethics and data protection. Furthermore, the government wishes to consolidate cyber diplomacy by setting up a cyber coordinator function in the Ministry of Foreign Affairs. The aim of this coordinator function is to increase Denmark's level of involvement in international collaboration on cyber security.

Furthermore, an initiative will be launched to reinforce export controls of cyber monitoring equipment. The focus here will be on ensuring clearer regulations and competent guidance from the authorities, such that Danish businesses will have the courage to focus on export and thereby develop a strong Danish cyber industry which may, at the same time, help bolster Denmark's cyber defences.

Initiatives – Joint Efforts

Initiative 3.1:
Sub-strategies at sectoral level and decentralised cyber-security units

In order to develop a stronger decentralised capability in the cyber and information security area, a sectoral unit will be established for each of the critical sectors. These units will contribute to threat assessments at sectoral level, monitoring, preparedness exercises, establishment of security systems, knowledge-sharing, instructions, etc. Furthermore, in 2018 a sector-specific strategy will be prepared for each of the critical sectors in continuation of the national strategy.

- **Initiative 3.1a:** Cyber and information security strategy for the energy sector
- **Initiative 3.1b:** Cyber and information security strategy for the healthcare sector
- **Initiative 3.1c:** Cyber and information security strategy for the transport sector
- **Initiative 3.1d:** Cyber and information security strategy for the telecommunication sector
- **Initiative 3.1e:** Cyber and information security strategy for the financial sector
- **Initiative 3.1f:** Cyber and information security strategy for the maritime sector

Initiative 3.2: Cross-authority efforts to support cyber and information security in sectors that are of vital importance to society

A cross-ministerial task force will be established with experts from the Centre for Cyber Security, the Agency for Digitisation and the Danish Security and Intelligence Service. In a transitional phase, and by means of guidance and joint initiatives, the task force will assist critical sectors in designing their sectoral strategies, establishing decentralised cyber security units and exchange of experience, as well as preparing guidelines for the sector's work to establish contingency plans in the information security area.

Initiative 3.3: Management of suppliers of outsourced ICT services

In order to improve ICT security and security of supply for government authorities' critical ICT systems, stricter requirements will be introduced for all public authorities regarding their use in future contracts concerning requisite security measures and management provisions for vital ICT systems, and for the authorities' regulation of private-sector suppliers.

Initiative 3.4: Strengthened national coordination

The strategic coordination of the cyber and information security area must be strengthened. To this end, a national steering committee for cyber and information security will be set up. This steering group will be tasked with following up on the implementation of the strategy for cyber and information security, launching any supplementary initiatives and analyses and regularly discussing Denmark's national policy on information security. The Forum for Dialogue on Information Security (Dialogforum for informationssikkerhed) will become an advisory board comprising experts whose role will be to supply input to the implementation and follow-up on the cyber strategy and its initiatives.

Initiative 3.5: Strengthened level of involvement in international collaboration

The government will strengthen Denmark's involvement internationally by posting two cyber attachés to the Danish EU representation in Brussels, who will help protect Danish interests of a cross-cutting nature. The government will also expand the setup for the Danish tech ambassador in Silicon Valley with an advisor dedicated to cyber and information security, just as it will strengthen its cyber diplomacy efforts with the appointment of an international cyber coordinator in the Ministry of Foreign Affairs of Denmark. Moreover, Denmark will participate in the NATO Cooperative Cyber Defence Centre of Excellence in Tallinn and in the European centres of Excellence for countering hybrid threats in Helsinki. Finally, Danish efforts in the field of export controls on cyber-surveillance technologies will be consolidated so as to help Danish businesses navigate this area and to prevent malicious third parties from using technology developed in Denmark to spy on the nation.

Initiative 3.6: Evaluation of the state of cyber and information security

Periodic national analyses of the cyber and information security situation are required in order to inform the assessment of whether initiatives implemented have had the desired effect and take into account changes to the threat scenario. The periodic, national analysis examines the cyber and information security situation in Denmark from both a broad and an in-depth perspective. It will look at threats, risks, level of protection, initiatives implemented, organisation and coordination, and links between sectors etc.

Initiative 3.7: Overview of information worthy of protection

In order to protect information of significance for national security and consolidate the work of assessing information security risks, initiatives will be implemented to provide the necessary overview of information deemed worthy of protection. This overview will be used to determine specific levels of classification and security both specifically at government level as well as overall as regards the significance the information in question has for society.

Initiative 3.8: Information security architecture

In order to support the authorities in developing ICT solutions that can support their ability to guarantee the confidentiality, integrity, accessibility and resilience of systems and services, a joint public-sector information security architecture will be established which will include principles, standards, shared components and guidelines.

Initiative 3.9: National and international efforts to safeguard data ethics and protection of personal data

The Danish government will consolidate its efforts relating to data ethics at national level with respect to data processing by Danish businesses as well as at international level. At national level, business-oriented information and guidance material will be prepared on the rules governing responsibility, ownership and rights in connection with the use of data. Furthermore, an expert group has been set up which includes representatives from the Danish business community and which has been tasked with preparing general recommendations for data ethics. The government will also launch a separate strategy concerning protection of Danish citizens' personal data. At the international level, the government will identify data ethics and data protection as key focus areas for the Danish tech ambassador in Silicon Valley as a step towards improving its dialogue with major multinational tech companies.

Appendix

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

The cyber and information security work is organised 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.

General principles for the national crisis management system in Denmark

The principle of sectoral responsibility
The authority which has day-to-day responsibility is also responsible in the event of a major accident or natural disaster.

The similarity principle
The procedures and responsibilities that apply during normal day-to-day operations shall also, insofar as possible, apply in the crisis management system.

The subsidiarity principle
The emergency response tasks must, insofar as possible, be managed locally and as close to the affected citizens as possible, and accordingly at the lowest suitable and relevant organisational level.

The principle of co-operation
Authorities have a separate responsibility for collaborating and coordinating with other authorities and organisations about emergency response planning and crisis management.

The precautionary principle
In situations in which information is unclear or incomplete, the level of emergency preparedness should preferably be too high rather than too low. Furthermore, there should be possible to easily and quickly lower the level of emergency preparedness in order to prevent wasting resources.

Source: National Emergency Response Plan, 6th edition 2009

The principle of sectoral responsibility

Source: Clairification of Sector Responsibility for Ministries and Agencies. National Vulnerability Report

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.

2. Responsibilities and roles in connection with incidents of significance for cyber and information security

2.1. 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 Danish Centre for Cyber Security. Finally, the entity is responsible for any external communication concerning the incident.

2.2. 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/Centre for Cyber Security) may be activated.

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.

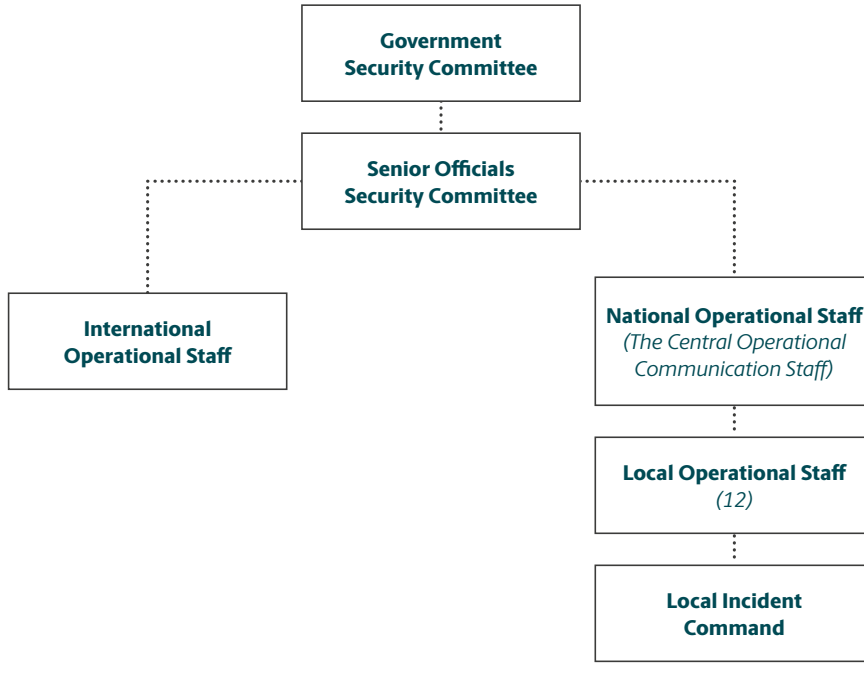
In connection with the majority of major cyberattacks there will be a need both for general investigations and technical, ICT-security investigations. To this end, close cooperation has been established between the police (including the Danish Security and Intelligence Service) and the Centre for Cyber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

2.3. 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 Danish 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

Figure 1
The Danish national crisis management system



Source: Crisis management in Denmark, the Danish Emergency Management Agency, 2015

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.

2.4. Recovery following a cyber incident

As a general rule, the affected entity (authority, business or organisation) is responsible for the recovery of commercial operations as well as ICT operations based on its incident response plan. The relevant unit may receive support from public or private vendors in the field and potentially also from the decentralised cyber security units in the individual sectors.

3. Regular coordination

The ongoing work on cyber and information security must be closely coordinated with, and subject to knowledge sharing between, the relevant authorities. To this end, a number of initiatives will be launched to support the work of the sectors and of authorities and businesses. These initiatives will also ensure closer national coordination in the field, particularly with regard to preventive work with ICT security.

The strategy stresses the requirement that sectors of critical importance to society establish a dedicated cyber and information security unit that can contribute to sector-specific threat assessments, vulnerabilities assessments, emergency response drills, security build-up, knowledge sharing, guidelines, etc.

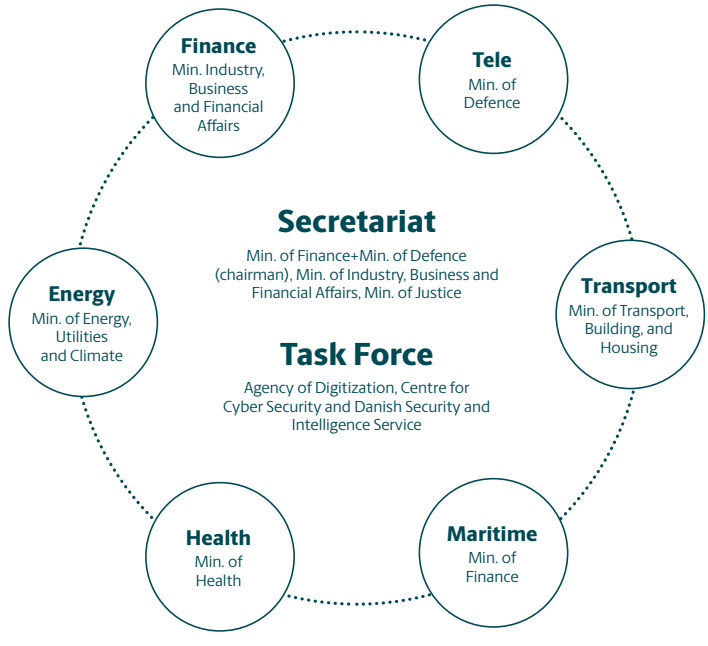


Figure 2
Steering committee for national cyber and information strategy coordination follow-up

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

Centre for Cyber Security
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.

Police
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.

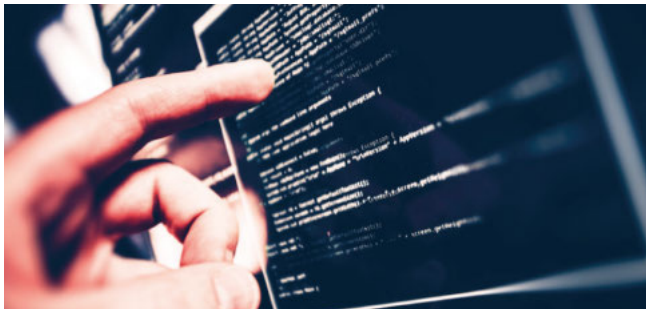
Danish Security and Intelligence Service
The Danish Security and Intelligence Service is the national security authority for Denmark and provides consultancy and assistance to public authorities and private businesses in security matters, including with regard to the human factor in information security, as well as physical security.

Agency for Digitisation
The Agency for Digitisation supports information security in the public sector and is responsible for a number of citizen-focused information tasks. The agency is also responsible for coordinating the implementation of the strategy in concert with the Ministry of Defence.

Danish Business Authority
The Danish Business Authority prepares information, guidelines and tools to strengthen the business community's work with ICT security and responsible data processing.

In order to strengthen the strategic coordination and implementation of the strategy, a national steering committee for cyber and information security will be set up to coordinate work across the individual sectors and link the work to national efforts in this area.

The requirement for sector-specific strategies and dedicated cyber and information security units in the individual sectors will ensure cross-cutting coordination within the individual sectors, as well as between sectors and national initiatives. A task force will be established comprising representatives from the Danish Agency for Digitisation, the Centre for Cyber Security and the Danish Security and Intelligence Service. Through advisory services and joint initiatives the task force will assist the sectors in establishing cyber information security units and in preparing sector-specific strategies.



4. 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.

4.1. Centre for Cyber Security

The Centre for Cyber Security was established in 2012 to ensure better protection against cyberattacks, etc. According to the Danish Defence Intelligence Service Act, the Danish Defence Intelligence Service is the national ICT security authority[1], and the service fulfils its responsibilities via the Danish Centre for Cyber Security.

With regard to proactive efforts, the Centre for Cyber Security provides advice to government authorities on cyber security, e.g. in connection with the procurement of new ICT systems. The centre also publishes guidelines on how to manage cyber security-related challenges. The threat assessment unit under the auspices of the Centre for Cyber Security prepares national and sector-specific situation reports and threat assessments.

With regard to reactive efforts, government authorities have the option of subscribing to the centre's infrastructure and Internet security service which ensures that the authority's Internet communication is monitored continuously for harmful traffic. In the event that a suspected cyberattack is detected, government authorities can contact the service for assistance, e.g. in the form of an on-site rapid response team.

The government has decided that all government authorities are required to report major ICT security incidents in their own ICT systems to the Centre for Cyber Security, such that the infrastructure and Internet security service has the most complete overview possible of the current security situation in the Danish part of the Internet.

The Centre for Cyber Security regularly issues situation reports and threat assessments. Unclassified situation reports and threat assessments are accessible via the Centre for Cyber Security's website at www.cfcs.dk. Classified threat assessments and warnings about specific cyber security incidents are forwarded directly to the authorities affected.

The 2018-2023 Defence Agreements will significantly enhance the ability of the Centre for Cyber Security to assist the authorities responsible for the relevant sectors. Strengthening of the Centre for Cyber Security will include reinforcing the centre's advisory and preventive roles and efforts to detect and issue warnings concerning specific incidents within critical sectors. This will be achieved by establishing a new national cyber situation centre which

[1] The Danish Security and Intelligence Service functions as the national ICT security authority with regard to the Ministry of Justice's area of responsibility.

will be manned 24-7. This centre will be tasked with operationalising information from intelligence sources, reported data, etc. and with preparing national situation reports concerning the current state of security for key digital networks.

4.2. The Danish Security and Intelligence Service

Pursuant to the Danish Security and Intelligence Service Act, the Danish Security and Intelligence Service is tasked with preventing, investigating and countering threats and actions that pose, or could pose, a danger to Denmark as an independent, democratic, safe and secure nation. The Danish Security and Intelligence Service's responsibilities cover the crimes set out in parts 12 (crimes against national security and national independence) and 13 (crimes against the Danish Constitution and against the supreme authorities, terrorism, etc.). This includes crimes which are directed at information and communications systems, or which involve the use of information and communication technologies.

Through its activities, the Danish Security and Intelligence Service shall contribute to identifying and managing threats of the kind set out above as early and as effectively as possible.

Furthermore, in its capacity as the national security authority, the Danish Security and Intelligence Service provides advice on the physical protection of sensitive information. This includes providing advice on security management with respect to employees who have physical access to information and information systems, as well as carrying out security evaluations and security authorisations. Finally, the Danish Security and Intelligence Service functions as the ICT security authority with regard to the Ministry of Justice's area of responsibility.

4.3. The police

Pursuant to the Police Act, the police are tasked with preventing and investigating criminal offences and with stopping criminal activities, including cases of IT-related crime.

In order to consolidate ICT-related crime management, in 2014 the Danish National Police established a national Cyber Crime Centre (NC3). With the exception of those tasks managed by the Danish Security and Intelligence Service, the Cyber Crime Centre has overall responsibility for determining the direction of police efforts to combat crime which targets ICT systems and crime that involves the use of ICT.

The police's jurisdiction encompasses all criminal offences punishable in Denmark. This includes actions carried out outside of Denmark if these actions infringe on Danish independence, Danish national security, violate the Danish Constitution or Danish government bodies, or if the effect of the criminal actions is intended to occur on Danish soil.

Furthermore, pursuant to the Emergency Management Act, the police have overall coordinating responsibility for the emergency response effort in situations involving major damage, including those which require the issuing of alerts, etc.

2017/18:35

May 2018

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

ISBN 978-87-93635-57-9 (pdf version)
ISBN 978-87-93635-48-7 (trykt version)

Design: e-Types
Photo: Ritzau Scanpix, Colourbox,
Johnér og Pexels
Print: Rosendahls

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

Ministry of Finance
Christiansborg Slotsplads 1
1218 Copenhagen K
Tlf.: +45 3392 3333