February 2015

The Danish Cyber and Information Security Strategy

1. Introduction

In December 2014 the Government presented a National Cyber and Information Security Strategy containing 27 government initiatives for 2015-2016.

Since its formation in 2011 the Danish Government has aimed to *strengthen protection against cyber-attacks while respecting the rule of law and personal freedom*. In Denmark, citizens and businesses must be able to trust that important functions in society are provided both efficiently and securely.

Digitisation, i.e. the extensive integration of digital technologies into society and the public sector, is a key element in the ongoing development of prosperity and welfare in the Danish society. It is crucial that the cyber and information security effort is professionalized and developed on a continuous basis. The digital infrastructure must be protected. This requires that cyber and information security is high on the agendas of management.

New challenges and threats have emerged. Hackers have succeeded in disturbing functions vital to society, or they have been able to access sensitive and valuable information. It is the assessment of the Danish Defence Intelligence Service that ICT-related treats to private citizens, businesses and government institutions are growing. Cyber-attacks against digital systems have become more widespread and more advanced. At the same time, government institutions face challenges when outsourcing parts of the infrastructure which important functions in society rely upon.

Denmark needs a strong protection against such threats as well as a strong reactive capacity. Extensive knowledge and understanding of the threats we face as a society is crucial. The present Cyber and Information Security Strategy therefore focuses on the need for more knowledge about security and the need for a professionalization of the day-to-day security effort of government institutions as well as cyber and information security in the telecom sector and the energy sector.

It is essential that the effort is integrated into the existing organizational structure so that the professionalization of the cyber and information security effort takes advantage of the knowledge that the authorities have of the areas they are each responsible for.

With the Cyber and Information Security Strategy the Government makes a significant step towards maintaining and reinforcing the confidence of businesses and citizens, ensuring that

Denmark is a safe country in which to invest and use digital services. Technological change will continue and we must likewise continually strengthen and adapt the security effort. The strategy will therefore be updated in late 2016 for a new period with the involvement of views and insights from interest groups, businesses and academia on how further efforts may most benefit society.

2. Strong and cohesive security

Digitisation is a global phenomenon that is rapidly changing Danish society at all levels. It has a strong impact on communication between citizens, businesses and government, and it influences the ways in which we arrange and organize our society.

Digitisation is no longer a choice; it is a premise. Danish businesses apply digital technology in production and internal processes – and increasingly in their products. In recent years, the Danish Government has implemented a series of digitisation strategies focused on administration, productivity and cooperation, services and welfare. The efficiency and innovation potential of digitisation is crucial to Denmark's competitiveness and prosperity.

With digitisation being a key component of public services and the functioning of society, the Government emphasizes the need for constant improvements in cyber and information security. With this strategy the Government aims to raise its cyber and information security effort through systematic application of the ISO27001 security standard, employing threat assessments and reinforcing ministries' ICT security oversight. Also, since much public ICT has been outsourced, services provided by external suppliers must be subject to a strong oversight. Security risk assessments of government IT projects is to be incorporated in the Cross-Departmental Programme Model and IT Project Model.

These measures are aimed at ensuring the professionalization of government institutions' day-to-day efforts regarding information security in order to improve resilience against cyber-attacks. The strategy contains several initiatives aimed at improving the understanding of threats and at systematically gathering experience from known cyber-attacks.

The strategy is aimed at government institutions but it also contains initiatives aimed at owners of infrastructure of vital importance to the provision of energy and telecommunications to the Danish society.

3. The challenge

The cyber and information security challenges are both technical and practical in nature.

Failure to comply with security routines. Part of the challenge is make government institutions ready to incorporate a systematic approach to information security in the daily routines. If the institutions do not set up the necessary information security routines and making concrete risk assessments regarding key systems the institutions risk overlooking security flaws and vulnerabilities.

Dynamic development. Cyber and information security threats are ever-changing and there are constantly emerging new threats that require the attention of the authorities. There is no indication that this will be less true in the years to come, quite the opposite. The efforts to address threats must therefore be continuously improved and renewed.

***Cyber threats*.** The Danish Defence Intelligence Service assesses that Danish government institutions, businesses and private individuals are the targets of daily attempts of harmful activity from various agents via the Internet. While public authorities are rarely seriously compromised, the threat from harmful activities is increasing. The Danish Defence Intelligence Service believes that the most severe cyber threats against Denmark come from foreign state-sponsored agents who seek to conduct espionage and steal Danish intellectual property and business secrets such as business plans, research results, technical know-how, financial information and contracts.

Insider threats. The so-called insider threats also pose a significant challenge. Insider threats include staff willfully or negligently breaching workplace security procedures. In this context, the threat of negligence poses a particular challenge – employees may inadvertently let unauthorized persons into the workplace by holding the door for strangers, or they may download programs with dubious contents. If the employees fail to observe security procedures, this increases the risk of unauthorized access to internal networks and therefore to sensitive information.

Balanced security
Information security initiatives must be adjusted to suit the diverse needs of the different government institutions and must reflect a careful balancing of *security, usability and economy*. The security effort should be proportional to the threat in question. Security must not be given precedence at all cost or unduly degrade the user experience and effectiveness of any given digital service. Security efforts must start with an assessment of the specific need for a given level of security. The individual authorities should therefore adopt a risk-based approach to security.

Supplier management. The Government also faces a number of threats in connection with the outsourcing of ICT operations. Government institutions must upgrade procedures to ensure that external suppliers observe the security procedures. The importance of such procedures is illustrated by the severe attack against the IT service provider CSC in 2012.

4. Stronger government effort

The Government has already introduced a number of initiatives aimed at strengthening the cyber security of the state, and it is monitoring government institutions' efforts. In particular, efforts of authorities with cyber security-related responsibilities have been stepped up.

The Government has established the Centre for Cyber Security under the Danish Defence Intelligence Service. The main mission of the Centre is to support the reinforcement of IT systems and infrastructure which important functions in society rely upon against external cyber threats.

Furthermore, the Government has established the Agency for Digitisation under the Ministry of Finance in order to combine activities related to state digitisation efforts. The mission of the Agency for Digitisation is to ensure professional and cohesive IT governance in developing cross-public sector digital infrastructure. The Agency also advises government institutions on the mandatory principles of information security management according to ISO27001.

The Danish police have set up the National Cyber Crime Center (NC3) whose mission is to prevent and investigate IT crime conducted online.

Combined, these actions enable government institutions and businesses with IT systems and infrastructure which important functions in society rely upon to further strengthen their cyber and information security. Therefore, the initiatives in the Cyber and Information Security Strategy build upon an already improved effort.

5. Strategic objectives

Overall, the Government's efforts to enhance cyber and information security efforts aim to:

- Maintain citizens' and businesses' trust that cyber and information security measures of government institutions and providers of IT systems and infrastructure which important functions in society rely upon are professional and satisfactory. Meanwhile, efforts to strengthen cyber and information security must permit user-friendly and effective use of new technologies.

- Strengthen the protection of important functions in society and national security against cyber-attacks.

To support these objectives, the government has identified six strategic focus areas to be targeted with specific initiatives to raise the cyber and information security level of the Danish society.

Professionalized and reinforced ICT oversight

- Ministries must manage information security systematically and professionally and initiate strong ICT oversight of subordinate authorities.

Clear guidelines for suppliers

- Government institutions must set clear requirements regarding cyber and information security for suppliers providing IT services and infrastructure, perform regular risk assessments and follow up regularly on providers' ICT security measures.

Strengthened cyber security and more knowledge

- Public sector cyber security levels must be raised and government institutions and business must have access to threat assessments and to advanced knowledge about how to reduce vulnerabilities.

Robust infrastructure in the energy and telecommunications sectors

- There must be a high level of cyber and information security within the energy and telecommunications sectors.

Denmark as a strong international partner

- Danish authorities must work with international partners to strengthen cyber and information security through active participation in relevant forums.

Strong investigation and high level of information

- Cyber-crime investigations must be strong and competent, and citizens and businesses must be given a better basis for adequately assuming responsibility for security in relation to their own equipment and online conduct.

The initiatives aim to ensure the maintaining of adequate security levels and will serve to significantly enhance Danish cyber and information security efforts. It is however important to stress that complete protection against breakdowns, compromise and other security incidents is unattainable.

Cyber and information security threats are ever-changing and efforts to ensure a high level of security must be continuously improved and renewed. Government institutions and suppliers must adopt a risk-based approach to security and embrace a focused and systematic approach, giving priority to the efforts that provide the strongest security balanced against the use of resources and the requirements for user-friendliness of public ICT services.

6. Strategy limitations

The Cyber and Information Security Strategy focuses on government institutions' cyber and information security efforts and launches a coordinated and long-term government effort which must be further developed and supplemented in various state sectors. Professionalizing the government's cyber and information security effort is essential to the protection of digital infrastructures which important functions in society rely upon.

The strategy is furthermore focused on cyber and information security within the energy and telecommunications sectors where private companies own and support a large part of the infrastructure. The motivation behind this particular focus is that the telecommunications sector forms the backbone of communication in modern society and that the energy sector provides the energy required to keep modern society running.

In parallel with this strategy, the Government, regions and municipalities have agreed to further increase information security efforts to protect privacy and to ensure a high level of security in the digital infrastructure at all levels of national and local government. The Government expects to extend this cooperative effort as part of the next eGovernment Strategy in which information

security will be a focus area. The strategy is jointly prepared by national and local authorities and slated to be launched in 2015. The Agency for Digitisation, regions and municipalities will assess whether additional efforts are required with regard to the implementation of ISO27001 once the effects from the Cyber and Information Security Strategy may be assessed.

The Government intends to update the Cyber and Information Security Strategy in late 2016. The update will be based on an assessment of the early effects of the present cyber and information security strategy, including follow-ups on each initiative, and identify areas where further action is relevant. The update will therefore include further relevant sectors in society, e.g. the financial sector.

An overview of the 27 initiatives in the strategy is given below.

Strategic goals: Strong and cohesive security					
• Citizens and businesses must be able to trust that the cyber and information security measures of government institutions and providers of IT systems and infrastructure are professional and reassuring. • The protection of key functions of society and of national security against cyber-attacks must be reinforced.					
Six focus areas					
Professionalized and reinforced ICT oversight	**Clear guidelines for suppliers**	**Strengthened cyber security and more knowledge**	**Robust infrastructure in the energy and tele-communications sectors**	**Denmark as a strong international partner**	**Strong investigation and high level of information**
Initiatives					
1. Increased information security effort in government institutions. **2.** Mandatory security risk assessment of public IT projects **3.** Increased coordination of information security efforts between national and local authorities **4.** Cooperation between education and research institutions regarding cyber and information security **5.** Intensified dialogue between private and public employers and education and research institutions regarding competence needs **6.** Sufficient capacity in the Agency for Governmental IT Services to handle cyber attacks	**7.** Introduction of security requirements in IT tenders and contracts **8.** Continuous security oversight of suppliers	**9.** Mandatory inclusion of cyber threats in government institutions' risk management **10.** Formation of a cyber-threat assessment unit **11.** Study regarding the possible concentration of government Internet connections **12.** Study regarding the development of secure communication among state institutions **13.** Formation of a unit to investigate major cyber security incidents **14.** Formation of a SCADA knowledge centre **15.** Setting up a business advisory board on ICT security	**16.** Strengthening of network and information security in telecommunications **17.** Stronger requirements regarding cyber and information security in the energy sector	**18.** Strengthening of Danish cyber diplomacy **19.** Promotion of Denmark's stance in international cyber and information security cooperation forums **20.** Nordic cooperation on research and education in cyber and information security	**21.** Raised security awareness among citizens and businesses **22.** Security self-check service for businesses **23.** Expansion of the National Cyber Crime Center (NC3) **24.** Increased capacity of the police regarding information security guidance **25.** Strengthening the cyber capacity and capability of the Danish Security and Intelligence Service (PET) **26.** Establishment of an online-platform for reporting cyber crime **27.** Study regarding a service providing information on stolen identity documents