DANMARKS NATIONALBANK

1 MARCH 2017 — NO 3

Cyber Resilience in the Financial Sector

In the worst case, severe cyberattacks may pose a threat to financial sector stability. In 2016, Danmarks Nationalbank and the Danish Financial Supervisory Authority therefore conducted a questionnaire survey of the cyber resilience of core financial sector participants in Denmark. The survey comprises major banks and mortgage banks as well as infrastructure companies providing critical services to these banks.

The survey of the cyber resilience of core financial sector participants in Denmark shows the following:

- The core financial sector participants in Denmark have strong focus on cyber security, but there is room for improvement.
- When cyber security is anchored in the top management, the level of cyber resilience is higher.
- Educating and training all employees in cyber security is essential.

Focus

Strong focus on cyber security but room for improvement

Read more

Management

Anchoring of cyber security in the top management

Read more

Education

Education of employees in cyber security

Read more

CONTACT

Karsten Biltoft
Assistant Governor and head of Financial Stability

kbi@nationalbanken.dk
+45 3363 6101

FINANCIAL STABILITY

Results of the survey

Strong focus on cyber security, but room for improvement

A survey conducted by Danmarks Nationalbank and the Danish Financial Supervisory Authority shows that the core financial sector participants in Denmark have strong focus on cyber security.

The core financial sector participants comprise systemically important banks and mortgage banks as well as infrastructure companies. The infrastructure companies include payment and settlement systems that are critical for banks and mortgage banks to be able to settle payments and securities transactions, as well as shared data centres that handle the operational management for many banks, mortgage banks and payment and settlement systems.

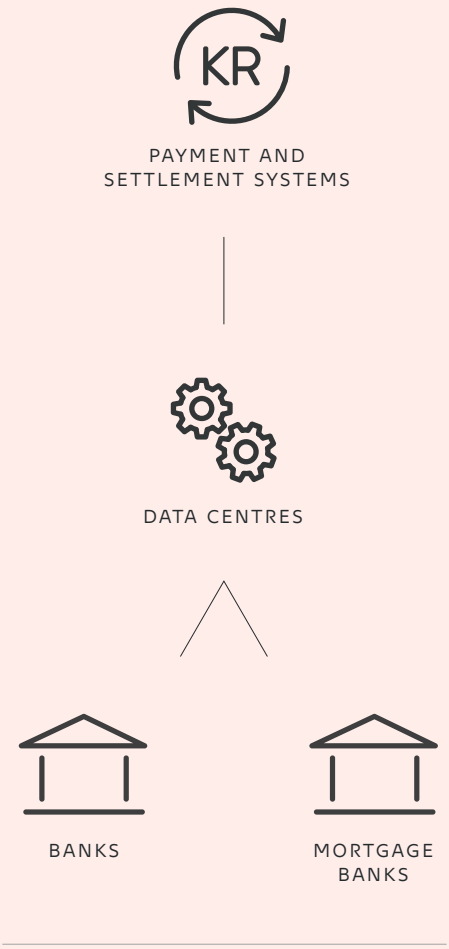
The level varies considerably among the 15 respondents to the survey, and most of them have room for improvement. The general picture is based on a questionnaire survey in which the participants themselves indicated their overall level of cyber resilience. Details of the questionnaire are provided in Box 2.

Cyber resilience is greater where the top management is involved

Cyber security is not a technical issue of relevance to a limited group of employees, e.g. in the IT department, since cyberattacks may have serious implications for the entire business. It affects everyone in the organisation from the board of directors to the staff.

Payments infrastructure

Core financial infrastructure participants took part in the survey



Cyberattacks Box 1

Cyber risk is the risk of external electronic attacks aimed at IT activities, including computers, servers, systems, networks, services, etc. A cyberattack typically seeks to find and exploit vulnerabilities of IT systems, internal procedures or employees.

A cyberattack may have the following direct effects on the IT systems of financial institutions and payment and settlement systems:

- *Availability*: Websites, online banking and critical business systems for settlement of transactions are disrupted, and time-critical payments may be delayed.
- *Confidentiality*: Confidential data may be shared with unauthorised persons or disclosed to the public.
- *Integrity*: Data may be compromised.

A cyberattack that hits a large financial institution may reduce confidence, which in turn may lead to investor or depositor flight. If a critical payment or settlement system is hit it can paralyze the entire or essential parts of the financial sector for a period of time. A cyberattack could therefore potentially jeopardise financial stability. Read more about cyber risk in Danmarks Nationalbank, *Financial stability*, 1st Half 2016, Chapter 5 (link).

The survey shows that the focus on cyber security is strongest among the financial sector participants with a cyber strategy approved by the board of directors and widely known in the organisation – i.e. involving the top management, other management levels and the employees alike. Generally, the level of cyber security of these participants is also higher in other areas, suggesting that the cyber security strategies are widely implemented in their organisations. The survey shows that the financial sector participants with a cyber strategy approved by the board of directors are also better at training their staff in cyber security and that they test their crisis response plans specifically against cyber incidents far more frequently.

The management can support the work regarding cyber security through requirements and expectations for the firm's cyber security work. The purpose of requirements and expectations is to specify how the firm identifies, manages and handles cyber-related risks. But the strategy must also become established throughout the organisation among employees at all levels. Furthermore, the level of cyber security can be strengthened and maintained by the performing levels focusing on the use of measurements and controls as the basis for their reports to the management, allowing the management to use what they learn from the feedback received to adjust the objectives and requirements they have laid down.

Involving the entire organisation may be a major change that requires making an effort to succeed and the top management leading the way.[1] In order to support the implementation of a cyber security strategy, it is important to use efficient measures such as presenting the need for change in a way that appeals to different types of employees, providing good role models, providing feedback to managers on how they come across as role models, building the skills employees need to implement the changes and seeing that they have time to incorporate the changes in practice.[2]

Structured mapping of cyber risks is necessary
Risk management is an ongoing process to identify, assess and manage risks. As part of good IT security and as a basis for establishing an effective strategy for managing cyber risk, structured mapping of critical business areas and their underlying systems and processes is required.

Moreover, specific risks must be identified in sufficient detail to enable a decision on how to address each risk. Formally identifying risks considerably increases the probability that they will be handled appropriately. Appropriate handling implies that the organisation protects itself against risks, prepares to detect whether risks materialise and draws up and tests plans for restoring operation if risks have resulted in an incident. The responses to the questionnaire show clear consistency between the respondents whose risk assessments specifically identify cyber risks and the respondents who test their crisis response plans against cyber incidents, for instance.

Finally, results from the day-to-day work regarding cyber risks, i.e. controls, incidents, etc., should be continuously incorporated in the management of cyber risks within the organisation to optimise the performance.

All employees should receive cyber security training
Cybercriminals increasingly use e.g. spear-phishing targeted at individuals in an organisation.[3] Spear-phishing is attempts to induce targeted individuals to reveal confidential information to be used for fraudulent purposes, e.g. via e-mail or a website. Thus, the employees of an organisation are potential access points for cybercrime, however secure the organisation's IT systems may otherwise be, and that is why all employees should receive ongoing training in good cyberspace conduct, e.g. handling of e-mails and USB sticks.

For employee groups with critical functions and access to the organisation's sensitive data, the risk of being exposed to cyberattacks is particularly high.

1 Surveys show that only 3 out of 10 projects for change become successfully anchored in the organisation implementing the change.

2 Extensive literature exists on change management. See e.g. Scott Keller and Carolyn Aiken, *The Inconvenient Truth About Change Management. Why it isn't working and what to do about it*, McKinsey & Company, 2008.

3 Cf. e.g. Danish Defence Intelligence Service, *Intelligence Risk Assessment 2015* (link) and Centre for Cyber Security, *Sikkerhedsvejledning: Spear-phishing – et voksende problem* (Security recommendations: Spear-phishing – a growing problem – in Danish only) (link).

Cyber resilience in the financial sector

Box 2

The questionnaire survey on the cyber resilience of key financial sector participants was conducted in 2016 under the auspices of the Financial Sector forum for Operational Resilience, FSOR[1], which is a forum for collaboration between authorities and key financial sector participants in Denmark. A modified version of a questionnaire developed by the Bank of England (link) was used. The questionnaire provides an overall picture of the following areas:

- Governance and management
- Identification of risks
- Protection against cyber risks
- Detection of cyber incidents
- Response to cyber incidents and recovery of operation.

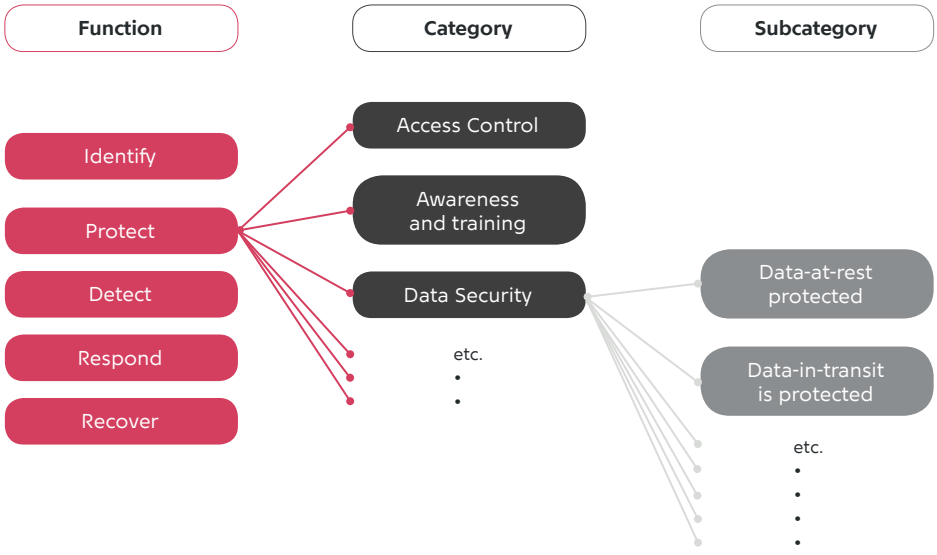
The questionnaire contains primarily closed questions, with possible answers ranging from an informalised ad hoc approach to cyber security to a formalised, consistent and risk-based approach where the organisation regularly adjusts itself. A similar grading of cyber security is available in e.g. NIST Cybersecurity Framework Tiers, which defines four cyber security tiers with an increasing degree of refinement and complexity in terms of organisations' management of cyber risk at each tier.

The above five areas of the questionnaire are part of various cyber security standards, cf. e.g. NIST Cybersecurity Framework (link), CPMI-IOSCO Guidance on cyber resilience for financial market infrastructures (link) and G7 Fundamental elements of cybersecurity for the financial sector (link).

Especially the CPMI-IOSCO Guidance emphasises the importance of ensuring that the top management is involved in maintaining appropriate cyber security and responsible for anchoring the cyber security work throughout the organisation and with service providers.

The NIST Cybersecurity Framework provides guidance on how critical infrastructure organisations can manage cyber risks and build up their cyber security. The framework core provides a set of functions (activities): "Identify", "Protect", "Detect", "Respond" and "Recover". The functions are broken down further into categories and subcategories to achieve a detailed operational level. Chart B.1 exemplifies the breakdown into subcategories.

NIST Cybersecurity Framework Core



Source: NIST Cybersecurity Framework (link).

1. For more information on the FSOR, see www.nationalbanken.dk (link).

Such employees are especially attractive targets for hackers seeking to install malware on IT equipment or to capture passwords, etc. These employees should therefore pay particular attention to cyber-attacks, and the organisation could benefit from giving them additional cyber security training.

The survey shows that half of the respondents to the questionnaire do not consistently train all employees in cyber security. A third of them provide special training for high-risk employees.

Testing crisis response plans against cyber incidents

As cyberattacks may have special characteristics compared to other operational incidents, it is important to test an organisation's crisis response plans specifically against cyber incidents. For instance, these special characteristics include that new types of attacks are constantly being developed, they may be harder to detect, their duration may potentially be considerably longer than for other types of operational incidents, and they may affect otherwise technically independent operating centres simultaneously.

Testing of crisis response plans is generally a useful tool for developing and improving the plans. It is essential that test results and results from other sources are regularly reported and incorporated in the work regarding cyber security.

It may be especially instructive to perform comprehensive testing of all crisis response plans together to check that all parts of the plans are interacting and not only working individually. An actual cyber incident could impact several areas at the same time. The questionnaire survey shows that about half of the respondents had not tested their crisis response plans against a cyber incident. While half of the remaining respondents had tested their plans together, the other half had only tested parts of their plans separately.

In order to benefit fully from testing crisis response plans against cyber incidents, the organisation needs to have a strong basis comprising the anchoring of cyber security measures at both management and staff levels, a formalised risk management programme as well as tools to detect cyberattacks.

DANMARKS NATIONALBANK
HAVNEGADE 5
DK-1093 COPENHAGEN K
WWW.NATIONALBANKEN.DK

Søren Truels Nielsen
stn@nationalbanken.dk

Katrine Skjærbæk Rasmussen
ks@nationalbanken.dk

FINANCIAL STABILITY

DANMARKS NATIONALBANK