DANMARKS NATIONALBANK

6 SEPTEMBER 2018 — NO. 12

Cyber resilience in the financial sector

Cyber resilience level has been improved

In a questionnaire survey, most of the core financial sector participants have reported that their levels of cyber resilience have been raised compared to 2016. A few have not improved their level and should give higher priority to their cyber effort.

Read more

Room for further improvement

For all respondents there is still room for improvement in some areas. This applies, for example, to mapping of critical business areas, where several financial sector participants could benefit from including the underlying information assets, systems and data more regularly in the mapping.

Read more

A high cyber threat level

The level of threat is expected to remain high in the coming years. So it is important that the efforts to ensure the cyber resilience of the financial sector continue to match developments in the cyber risk landscape. Danmarks Nationalbank will monitor developments closely and perform similar surveys of the core participants' levels of cyber resilience.

Read more

Survey of cyber resilience in the Danish financial sector Box 1

In the worst case, severe cyberattacks may pose a threat to financial sector stability. One of Danmarks Nationalbank's main objectives is to contribute to the stability of the financial system. Therefore, Danmarks Nationalbank and the Danish Financial Supervisory Authority have conducted a questionnaire survey of the cyber resilience of the core financial sector participants in Denmark in 2018. The survey follows up a similar survey from 2016 and comprises major banks and mortgage banks as well as key financial infrastructure companies.

Cyber resilience has been improved

Overall, the core financial sector participants have assessed their level of cyber resilience to be higher compared with the 2016 level[1]. That is one of the main findings of a new questionnaire survey conducted in the spring of 2018. The procedure is described in Box 2. As in 2016, the systemically important banks and mortgage banks as well as central infrastructure companies participated in the survey. The infrastructure companies include payment and settlement systems that are critical to banks' and mortgage banks' execution of payments and securities transactions, as well as shared data centres that provide operational services to many banks, mortgage banks and payment and settlement systems.

Generally speaking, the results of the survey show that the level of resilience has improved considerably compared with the 2016 results. For some of the respondents, there are significant improvements within all categories, while most report improvement on some parameters and they should therefore prioritise their efforts in selected areas. A few have not improved and should give higher priority to their cyber effort.

In 2016, Danmarks Nationalbank recommended a number of actions to be taken by some of the respondents: establishing a board-approved cyber strategy, training all employees in cyber security, testing contingency plans against cyber incidents, and taking a structured approach to mapping of cyber risks. The results of the survey indicate that progress has been made in relation to all recommendations, but to varying degrees.

A higher level of resilience if top management is involved

The survey shows that most respondents now report that they have a cyber strategy that has been approved by their board of directors. This is positive, and the results also show a clear tendency for participants with a board-approved strategy to have a higher level of cyber resilience in other areas. So management can use the strategy to step up cyber security efforts as the strategy includes requirements and expectations for identifying, managing and handling cyber risks.

The replies from the respondents also point out that most of them conduct effectiveness measurements to assess whether their cyber resilience targets are met. These measurements are important management tools for assessing the adequacy and effectiveness of cyber security efforts.

More respondents are offering employees cyber security training

Most respondents state that all employees receive regular awareness and cyber security training. The employees of an organisation are potential access points for cybercrime, no matter how secure the organisation's IT systems are. Cybercriminals often employ tactics that are targeted at individuals within an organisation. The attacks typically take place via phishing emails or through infection of websites visited by the victim. So there should be increased focus on special training of high-risk employees and follow-up on the effects of the training.

1 The main conclusions of the 2016 survey can be found in Danmarks Nationalbank, Cyber resilience in the financial sector, *Danmarks Nationalbank Analysis*, No. 3, March 2017 (*link*).

Questionnaire survey on cyber resilience in the Danish financial sector

Box 2

In the spring of 2018, Danmarks Nationalbank and the Danish Financial Supervisory Authority conducted a questionnaire survey of the cyber resilience of core participants in the Danish financial sector. This was the second survey of its kind in Denmark; the first one was conducted in August 2016. As in 2016, a modified version of a questionnaire developed by the Bank of England (*link*) was used. The questionnaire is based on various cyber security standards, such as the NIST Cybersecurity Framework (*link*), the CPMI-IOSCO Guidance on cyber resilience for financial market infrastructures (*link*) and the G7 Fundamental elements of cybersecurity for the financial sector (*link*). The questionnaire contains questions relating to the following five categories:

1. Governance
2. Identification of risks
3. Protection against cyber risks
4. Detection of cyber incidents
5. Responding to cyber incidents and restoring operations.

The results provide an indication of the overall maturity level of the sector

The questionnaire includes closed questions with responses (A, B or C) ranging from a non-formalised ad hoc approach to cyber security to a formalised, consistent and risk-based approach where the organisation is constantly adapting. The respondents themselves assess their levels within the five questionnaire categories, and the results provide an indication of the maturity level. This analysis focuses on the status and development of and variation in respondents' maturity levels.

Far more respondents are testing their measures against cyber incidents

The 2018 survey shows that since 2016 there has been a strong increase in the number of participants that are testing contingency plans against cyber incidents. A cyberattack at a systemically important bank, mortgage bank or central infrastructure company that seriously affects the availability of systems or the integrity of data may rapidly impact on the entire financial system in Denmark. Cyberattacks can have special characteristics compared with other operational incidents. For example, they may be of significantly longer duration than other operational incidents, and several technically independent operating centres may be affected at the same time. So it is important that the core participants test their ability to restore operations quickly, efficiently and securely.

In 2016, the Fincial Sector forum for Operational Robustness, FSOR, (*link*) established financial sector crisis response plans with a view to managing serious operational incidents, including cyberattacks. The purpose of the crisis response plans is to ensure a coordinated cross-sector effort in order to minimise the scope and consequences of a crisis. The crisis response plan was most recently tested in the autumn of 2017.

Structured mapping of cyber risks

The survey shows that respondents with a structured approach to mapping of cyber risks also have a higher overall level of security when it comes to protecting themselves against, detecting and responding to cyber incidents. Structured mapping of cyber risks is an important prerequisite for developing an effective cyber risk management strategy. This requires a formalised and consistent approach, and the organisation must continuously respond to developments in the risk scenario. A non-formalised and inconsistent approach could mean that specific risks are not identified in time or at a sufficiently high level to allow decisions to be made on how to prioritise and handle measures to counter the individual risks.

Room for further improvement

A high level of cyber resilience requires a continuous effort, and there will presumably always be room for improvement in some areas. In addition, organised cybercrime groups and state actors have increased their capacities compared to 2016, which underlines the need to continuously improve the effort to maintain and raise the level of resilience. With this in mind, the survey shows that most respondents assess that their overall level of cyber resilience has been increased, but also that more can be done. The few who have not yet followed up the recommendations from 2016 are encouraged to do so as soon as possible. The survey points to a number of areas that should be prioritised if an even higher level of cyber resilience is to be achieved. Examples have been provided below.

Mapping critical business areas
A key prerequisite for identifying risks is to perform detailed mapping of critical business areas and the processes that support these areas on a regular basis. It is also important that participants prepare and continuously maintain an indicative definition of normal network activity and data traffic.

The survey shows that most core participants have established a routine process for mapping critical business areas. But it also shows that underlying information assets, links between systems and data are not always included in the process on a regular basis. In a worst case scenario, this could mean that significant vulnerabilities are overlooked and not included in the risk management. Participants are therefore encouraged to include the necessary information assets, etc. in the mapping process on a structured basis.

New tools for detecting hacker attacks
The rise in sophisticated cyberattacks underscores the importance of using tracking tools that can detect actual incidents as early as possible. Consequently, use of automated tracking tools should be increased. Automated tracking tools can detect irregularities in normal network activity and data flows by means of e.g. analyses based on artificial intelligence.

In connection with the above, regular vulnerability scans and penetration tests, i.e. technical attempts to penetrate critical systems, should still be performed. These are essential tools in the effort to detect and disclose potential weaknesses in the defensive systems.

Penetration testing can be complemented by other tools that to a larger extent test the ability to detect and respond to attacks that have already materialised. One option is a "red team" test that simulates the techniques, tactics and procedures currently applied by sophisticated hacker groups. In early 2018, Danmarks Nationalbank and the core financial sector participants agreed to establish a Danish red team test programme. Its establishment was announced in a press release from Danmarks Nationalbank on 8 February 2018 (*link*). It is important to use a wide range of tools to detect sophisticated hacker attacks such as an Advanced Persistent Threat, which may have a long "incubation period" and be difficult to detect.

The cyber threat level remains high

The threat from cybercrime and cyberespionage against the Danish financial sector is high. This is the assessment in the Centre for Cyber Security's report: "Cyber Threats to the Financial Sector" from 2018 (*link*). The majority of financial sector participants also point out that cyber risk is the single risk that could potentially have the greatest impact on financial stability in Denmark in the next three years, cf. Box 3. However, according to Centre for Cyber Security it is less likely that foreign states will conduct destructive cyber attacks against the financial sector.

Overall, there is a need for the sector to continue to focus on developing and improving the level of cyber resilience so that it always matches the cyber risk landscape. This is why Danmarks Nationalbank will continue to monitor cyber developments closely in the coming years and perform further surveys of cyber resilience levels.

Cyber risk and the financial sector

Box 3

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 weaknesses in 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:* Critical business systems are disrupted.
- *Confidentiality:* Data may be shared with unauthorised persons or disclosed to the public.
- *Integrity:* Data may be compromised.

In recent years, there have been several international examples of advanced attacks from state-supported hacker groups targeted companies in the financial sector. There have been several attacks where banks' systems have been compromised resulting in unauthorised payments via data networks for interbank payments, such as the SWIFT network. In addition, there have been examples of attacks that have managed to spread malware to more than 100 different financial companies in more than 30 countries, cf. the Centre for Cyber Security Threat Assessment for the Financial Sector from 2018 (*link*).

A survey performed by the Danish Financial Supervisory Authority in May 2018 shows that cyber security is the risk which most financial enterprises believe may affect financial stability in Denmark in the next three years.[1] Several respondents specifically mention the risk of attacks on major financial institutions and the financial infrastructure's payment and settlement systems. A few mention limited resources and focus on cyber security as risk factors. Besides the direct losses and damage associated with cyberattacks, respondents express concerns about a consequential loss of trust in the financial system.

1. See the Danish Financial Supervisory Authority, Systemisk risiko – spørgeskemaundersøgelse (Systemic risk – questionnaire survey – in Danish only), 31 May 2018 (*link*).

ABOUT ANALYSIS

As a consequence of Danmarks Nationalbank's role in society we conduct analyses of economic and financial conditions.

Analyses are published continuously and include e.g. assessments of the current cyclical position and the financial stability.

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

This edition closed for contributions on 5 September 2018

Johan Gustav Kaas-Jacobsen
Principal Infrastructure Expert

FINANCIAL STABILITY

DANMARKS NATIONALBANK