DANMARKS NATIONALBANK

1 SEPTEMBER 2021 — NO. 20

How cyber resilient is the Danish financial sector?

- Danmarks Nationalbank's surveys show that the level of cyber resilience is higher now than it was in 2018. Key financial sector participants have strong external defences and more tools to detect and respond to cyber attacks.
- The risk that sophisticated hacker groups will breach external defences cannot be eliminated.
- It is essential for the financial companies to strengthen their internal security defences, further protect critical data and continue to build their capabilities for safe and effective recovery of core systems following a cyber attack.

In severe cases, a cyber attack could cause a systemic impact and lead to financial instability. Because of the systemic risk, Danmarks Nationalbank examines financial sector cyber resilience – for instance by conducting a questionnaire-based survey which, based on the respondents' self-assessments, provides an overview of financial sector cyber resilience. The questionnaire provides inputs for initiatives to address the most serious cyber risks facing the sector. Participants may also use the survey results to benchmark themselves against the respondent group.

In summer 2020, Danmarks Nationalbank conducted its third questionnaire-based survey

In the 2020 survey, banks, mortgage credit institutions, data centres and infrastructure companies critical to society performed self-assessments of their current levels of cyber resilience. Similar surveys were conducted in 2016 and 2018. But the bar of the surveys has been raised in line with evolving risks. This means that questions and response options are aligned with the specific challenges facing the respondents. The form and content of the surveys are described in detail in box 1, and the overall survey results are presented below.

Progress in efforts involving organisation, strategy and governance

The 2020 survey responses indicate an improvement in the respondents' planning, organisation and implementation of cyber governance compared with the previous surveys. The vast majority of respondents indicate that the overall risk management strategy and framework are defined by the top management, that is the executive board and the board of directors. The cyber security threat potentially poses a risk to the business of financial undertakings.

Therefore, responsibility for defining the strategic focus and prioritisation of cyber resilience efforts naturally belongs at the top management level.

High level of cyber attack protection

Perimeter security, that is the capability to protect systems and networks against external cyber attacks, has historically been a keen focus area for the financial sector. One reason is that financial companies have been an obvious target for cyber criminals since the 1990s when digitisation was taking off. Therefore, long-term experience has been gained with the protection against attempted external cyber attacks.

The most recent survey results indicate that further progress has been made. As a case in point, it is positive that the respondents all indicate that multiple layers of security have been implemented to ensure that their companies' networks are effectively segregated[1] and protected. Also, all respondents now have formalised staff training programmes in place, aimed at raising good practice awareness to reduce the risk of compromising security.

More and better detection

Because the techniques and tactics applied by cyber criminals are constantly becoming more sophisticated, external system protection cannot stand alone. Experience from cyber attacks, both in Denmark and abroad, shows that the most advanced cyber threat actors have the resources, techniques, time and patience to breach the external defences of even well protected companies. This is exemplified by the SolarWinds Orion attack, described in box 2, which compromised the networks of several major companies across the globe. So, it is positive that the responses to questions involving oversight of systems and networks to detect anomalies indicate clear improvements compared with earlier surveys.

The responses indicate progress in efforts to create and maintain a baseline of network and system activity – a precondition for supporting effective detection to identify anomalies. Most respondents also indicate that they have implemented alerts in their detection systems. These alerts are directly linked to the incident response management, so if an alert is triggered, the response plans will automatically be activated.

Overall, system and network detection efforts are among the top areas of improvement of financial sector participants since 2018. It is essential that this trend is maintained to ensure continued progress. There is still potential for improvement, for instance in terms of the scope of systems and networks overseen and in terms of the updating frequency of the recognition patterns for detection.

Potential for improvement in management of cyber risk and information assets

The 2020 survey also indicates other potential areas of improvement. One such area is identification and assessment of cyber risks and management of information assets such as hardware, software, systems, data etc.

It is key that the systems, processes and data supporting business activities critical to society are identified, risk assessed and classified by criticality. As a minimum, all institutions should have a general overview of their information assets, for instance in the form of a single database.[2] The responses show that several respondents could stand to benefit from enhancing the systematics of information asset management, including tracking of expiration dates of all critical hardware and software. Expired assets that are no longer supported may have potential vulnerabilities. All respondents have formalised processes in place to follow up on hardware/software vulnerabilities, but some respondents could stand to benefit from increasing the follow-up frequency and systematics.

Need for increased focus on data protection and recovery efforts

In recent years, the complexity of cyber security has increased, reflected in several serious cyber attacks with critical implications, several of these in Denmark. In response to the evolution of the risk landscape, Danmarks Nationalbank decided to expand the 2020 survey to include a number of detailed

1 Network segregation involves the development and enforcement of a set of rules for managing traffic between the company's critical networks and other less sensitive networks, for instance the Internet.

2 One option is to set up a Configuration Management Database (CMDB system) for continuous updating and storage of information about hardware and software assets.

Danmarks Nationalbank's cyber resilience surveys

Box 1

Purpose and methodology
The purpose of the survey is to provide an overview of the current level of cyber resilience of key financial sector participants. Results are based on the respondents' self-assessments, and responses are not verified.

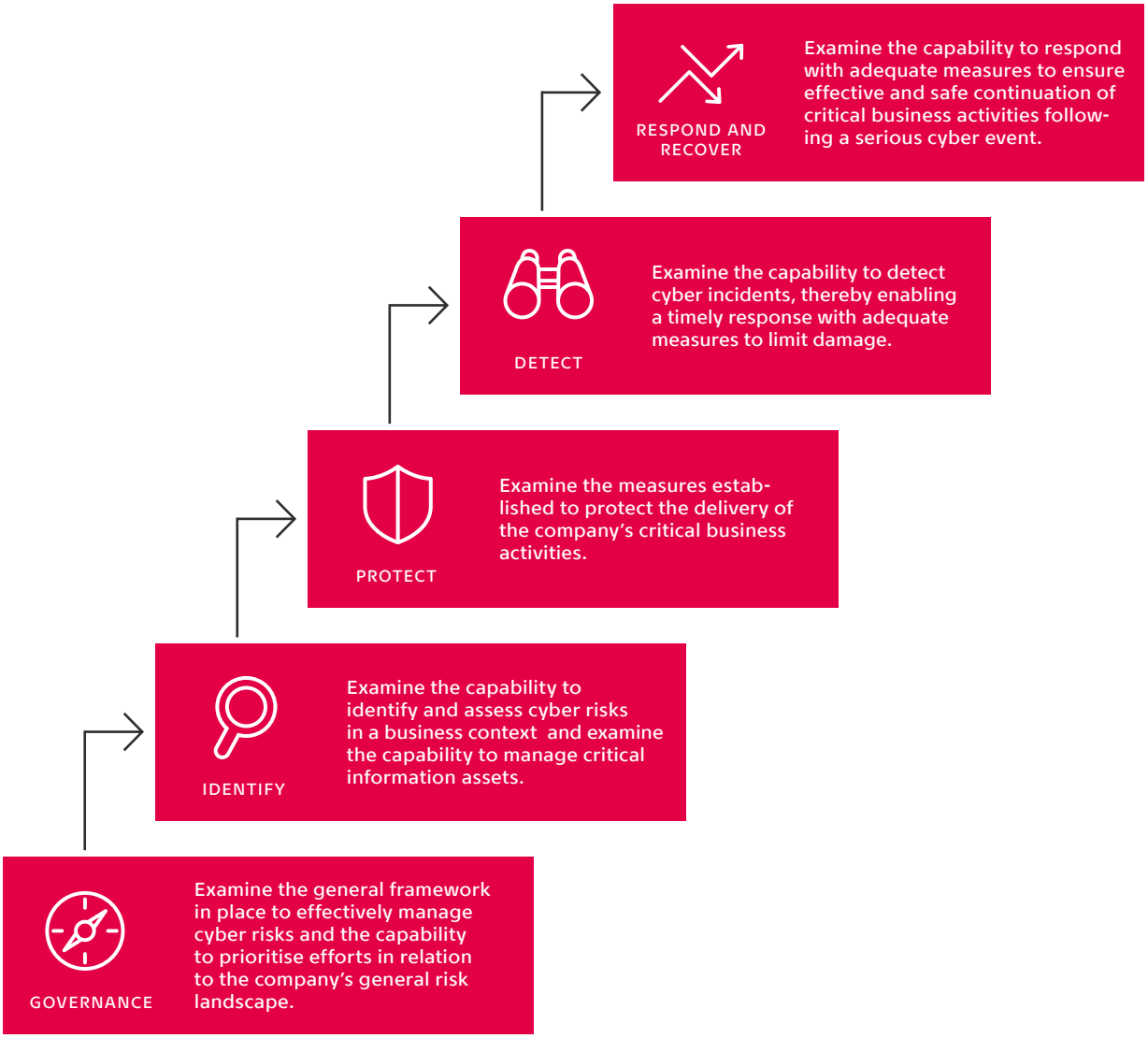
The questionnaire
Danmarks Nationalbank's surveys are based on an adapted version of a questionnaire developed by the Bank of England (*link*). The questionnaire contains questions related to five general elements of cyber resilience, described in more detail in the chart below.

Each question has four specific response options, depending on the degree of formalisation, consistency and risk of each organisation's approach to the item surveyed. A similar grading of cyber resilience is available in, for instance, NIST Cybersecurity Framework Tiers[1], defining four tiers of cybersecurity with an increasing degree of refinement and complexity of the organisation's cyber risk management.

In addition to examining the tier of each element, responses also indicate how each respondent works with cyber resilience.

Continues

Elements of the survey and their purpose



1. NIST Cybersecurity Framework is a US framework, setting standards and providing recommendations to organisations for ways to address cyber security, based on the experience of a wide range of companies from different sectors.

Danmarks Nationalbank's cyber resilience surveys
continued

Box 1

For instance, it is essential that each respondent, as one of the first things, has developed a cyber strategy approved by top management to ensure that the prioritisation and direction of their cyber resilience efforts are aligned with the company's general risk landscape.

In 2020, Danmarks Nationalbank decided to expand the questionnaire to include a number of detailed questions regarding the respondents' data security efforts and capabilities to ensure effective and safe recovery following a cyber attack. The reason was that earlier surveys showed that respondents had generally come a long way in establishing general frameworks and protecting their systems and networks. This left room for more detailed focus on special aspects, using a risk-based approach.

Participants
Systemically important banks, mortgage credit institutions, data centres and infrastructure companies participated in the surveys in 2016, 2018 and 2020, respectively. As a new feature, a group of insurance and pension companies and several key suppliers also participated in the latest survey.

The expansion of the group of survey participants allows for greater insight into the current tier of cyber resilience across various financial sector participants. This analysis, however, focuses exclusively on the responses of recurrent participants from the two earlier surveys.

questions regarding respondents' data security efforts and capability to ensure effective and safe recovery following a cyber attack.

Data protection and recovery are closely linked: if critical data are not available, this will substantially impact the systems' ability to restore operations. Encryption and backup are key elements of effective data protection. It is essential that the solutions used are closely aligned with the individual company's systems and infrastructure. If the storage – and therefore the protection – of data is handled by an external cloud or IT service provider, such alignment should be undertaken in close partnership with the external providers. Use of encryption and backup is also a source of derived risk that should be assessed and addressed. The purpose is to prevent the solutions used from causing vulnerabilities that may be exploited by malicious hackers.

When it comes to recovery, it is essential that all key participants have developed and maintain a targeted cyber contingency plan for recovery of systems and continuation of critical business activities following a cyber incident.

The response plan should be tested regularly using a risk-based approach based on extreme but plausible scenarios that could be caused by a cyber attack. Responses to the survey questions regarding data protection and recovery vary greatly, and the survey in general shows a need for increased focus on these areas. It is important that all key financial sector participants continuously seek to ensure that their current measures are aligned with the evolution of the risk landscape.

Broader operational resilience collaboration

The participants in the survey receive detailed feedback on their individual results. The organisations use this feedback to improve cyber security. Participants are also invited to attend workshops to exchange best practice knowledge.

All companies in the financial ecosystem are individually responsible for ensuring that their cyber resilience level is adequate and that they meet the requirements of applicable standards and regulations. This includes management of the risks each participant inflicts on other parts of the system.

Interconnectedness of technical and financial systems may cause cyber attacks to spread across financial sector institutions and systems. Moreover, due to their resource-intensive nature, some measures require joint action. So, on top of individual efforts, it makes sense – both from the perspective of the individual institution and the perspective of society – for the sector to collaborate on addressing cyber risks.

In 2016, this prompted Danmarks Nationalbank to take the initiative to set up Financial Sector Forum for Operational Resilience, FSOR[3], with the participation of key financial sector participants and authorities. FSOR meets twice a year to share knowledge, report progress on the workstreams along which FSOR works and decide on new initiatives. Between meetings, a number of working groups work on the initiatives agreed upon. FSOR's current workstreams include undertaking regular analysis of systemic risks, a joint sector crisis response and joint initiatives to improve the protection of critical sector data and enhance the capability to recover from an attack.

Danmarks Nationalbank's test programme TIBER-DK is another key element in financial sector cyber resilience efforts. TIBER, Threat Intelligence Based Ethical Red-teaming, is a red-teaming test procedure in which participants' live systems are tested by running simulated cyber attacks.

While the surveys provides a broad overview of financial sector cyber resilience, TIBER-DK pressure tests the individual organisation in practice. A TIBER-DK test is not passed or failed. The success criterion is for the learning outcome of each test participant to be high.

Considerable efforts are undertaken – both by individual institutions and jointly by the sector. The surveys provide an insight into how these efforts have improved the sector's cyber maturity.

Several examples of serious cyber attacks in recent years Box 2

Notable examples in Denmark include the June 2017 malware[1] attack on Maersk and the September 2019 and February 2020 ransomware[2] attacks against Demant and ISS, respectively, all of which disrupted, in full or the part, the companies' access to critical IT systems and data for a period of a week or more. These attacks had severe business implications and resulted in loss of revenue and expenses related to external recovery assistance. Between them, the three attacks cost the companies an estimated kr. +3 billion.

A number of cyber attacks have also been launched abroad, including attacks against the financial sector. For instance, the payment systems of Malta's largest bank, Bank de Valletta, were hit by a cyber attack in February 2019. The cyber attack against Bank de Valletta caused the bank to shut down all internal and customer-facing systems for 24 hours, including all its branches and ATMs.

In December 2020, it was revealed that a hostile actor had trojanised software updates of SolarWinds Orion, a network monitoring platform used by many large private companies and public organisations across the globe. The attack hit a key supplier in the Danish financial sector, but without any actual impact. The relevant systems were contained and analysed as soon as the compromised updates were known. The attack was not targeted at systems in the Danish financial sector, which may have helped to ensure that the incident could be resolved without any real damage.

Recently, the risk of supplier chain attacks came further to the fore when, in June 2021, Swedish supermarket chain Coop was forced to shut down virtually all its 800 stores in Sweden after it fell victim to a hacker attack against US software provider Kaseya. Coop did not use the compromised software, but was affected through the supplier providing the chain's till and checkout systems. Stores were closed for several days until the till and checkout issues were resolved.

1. Malware is malicious software specifically designed to disrupt, damage or gain unauthorised access to a computer system.
2. Ransomware is a specific type of malware designed to block access to a computer system until a ransom has been paid.

3 Find more information about FSOR on the Danmarks Nationalbank's website (link).

PUBLICATIONS

NEWS

News offers quick and accessible insight into an Analysis, an Economic Memo, a Working Paper or a Report from Danmarks Nationalbank. News is published continuously.

ANALYSIS

Analyses from Danmarks Nationalbank focus on economic and financial matters. Some Analyses are published at regular intervals, e.g. *Outlook for the Danish economy* and *Financial stability*. Other Analyses are published continuously.

REPORT

Reports comprise recurring reports and reviews of the functioning of Danmarks Nationalbank and include, for instance, the *Annual report* and the annual publication *Danish government borrowing and debt.*

ECONOMIC MEMO

An Economic Memo is a cross between an Analysis and a Working Paper and often shows the ongoing study of the authors. The publication series is primarily aimed at professionals. Economic Memos are published continuously.

WORKING PAPER

Working Papers present research projects by economists in Danmarks Nationalbank and their associates. The series is primarily targeted at professionals and people with an interest in academia. Working Papers are published continuously.

The analysis consists of a Danish and an English version. In case of doubt regarding the correctness of the translation the Danish version is considered to be binding.

DANMARKS NATIONALBANK
LANGELINIE ALLÉ 47
DK-2100 COPENHAGEN Ø
WWW.NATIONALBANKEN.DK

This edition closed for contributions on 25 August 2021

Gustav Kaas-Jacobsen
Infrastructure Advisor
joj@nationalbanken.dk
FINANCIAL STABILITY

DANMARKS
NATIONALBANK

CONTACT

Teis Hald Jensen
Communications
and Press Officer

tehj@nationalbanken.dk
+45 3363 6066

SECRETARIAT
AND COMMUNICATIONS