10 February 2022

# Progress in cyber resilience in 2021

FSOR

FINANCIAL SECTOR FORUM FOR OPERATIONAL RESILIENCE

## Progress in cyber resilience in 2021

2021 marked the fifth anniversary of the Financial Sector Forum for Operational Resilience. Since its establishment in 2016, the financial sector has worked together in a joint collaboration forum to increase the sector's operational resilience, including cyber resilience. The FSOR collaboration is a central forum where the sector can address key risks using its combined knowledge and resources. In recent years alone, cyberattacks against, for example, SolarWinds and Microsoft Exchange have shown that malicious attacks, e.g. via suppliers, can be sophisticated and have a widereaching impact.

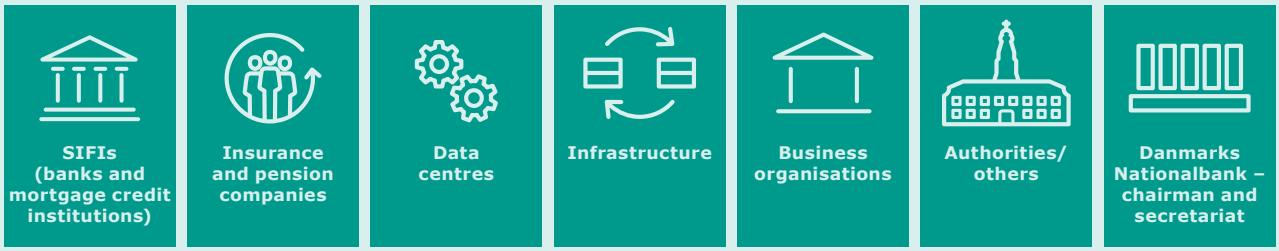
In 2021, FSOR decided to expand its membership with two new members in the form of Arbejdernes Landsbank and MasterCard. Furthermore, Peter Ejler Storgaard from Danmarks Nationalbank has taken over as new chairman, after the previous chairman resigned as part of a job change.

In 2021, FSOR especially focused on

- A sectorlevel risk analysis, which is updated every six months. Two new risks were added during 2021, bringing the total number of identified risks up to 41.
- Establishing the framework for identifying data that is critical to society with the aim of improving the sector's data protection and ability to recover in the event of an incident.
- Developing a concrete tool, Baseline, to assess the cyber resilience of the individual organisations and suppliers.
- Applying the results of a cyber survey to assess the individual organisation's status visàvis the rest of the financial sector as well as to exchange knowledge.
- Testing the sector's crisis management twice and updating the crisis management plan quarterly.
- Launching an evaluation of the framework for the FSOR collaboration through visits to the operational members.

These initiatives are described in further detail below. In addition, Danmarks Nationalbank and the financial sector have continued to work together on the TIBER programme – also with the aim of strengthening cyber resilience.

**The importance of FSOR's work on increasing the operational resilience is emphasized by sophisticated and malicious cyber attacks.**




## Financial sector forum for operational resilience

In 2016, the financial sector in Denmark established a privatepublic collaboration forum (the Financial Sector Forum for Operational Resilience (FSOR)) to increase the sector's operational resilience to cyberattacks, among other threats.

FSOR is a voluntary, yet binding, collaboration forum whose members are the core players of the financial sector. The FSOR members are:

- The largest and systemically important financial institutions, SIFIs, and representatives of insurance and pension companies.
- Data centres that operate critical systems and store and handle parts of the sector's data.
- The undertakings that own the infrastructure, including financial transaction platforms.
- Financial business organisations.
- Central authorities. Danmarks Nationalbank chairs FSOR and provides secretariat services.

FSOR focuses on the systemic risks that can threaten financial stability and the real economy, and sets the current agenda for the joint work with operational resilience in the Danish financial sector.

# FSOR collaboration expanded with two new members

At least once a year, the FSOR members assess whether all relevant players are represented in the forum. Arbejdernes Landsbank has been identified as a new SIFI following its acquisition of the

majority stake in Vestjysk Bank, and MasterCard has assumed responsibility for the operation of the retail payment system from Nets. Both organisations were therefore invited to join the FSOR collaboration.

## Risk analysis sets the direction for joint actions in FSOR

FSOR collaborates on identifying and addressing operational risks that could affect the entire sector and potentially threaten financial stability. Central to this work is a systematic risk analysis that contributes to identifying risks and provides a structured basis for prioritising measures to reduce risks.

A number of sources are used in risk analysis to identify the risks faced by the financial sector. This includes mapping key business processes and systemic dependencies, past incidents, threat assessments and input from FSOR members, including input from the annual survey of FSOR members' main concerns in relation to operational resilience. Danmarks Nationalbank has published the risk analysis method on its website (*link*).

The risk analysis is updated every six months. In the updates in 2021, two new risks were identified, bringing the total number of risks up to 41. The assessment of existing risks was revisited in relation to probability and consequence. In 2021, FSOR had a special focus on risks in relation to the protection of critical data and the recovery of data after a possible cyberattack.

Risks in the central infrastructure are discussed in more detail in the Risk Forum for Interdependencies, RGA, which is a collaboration forum with the participation of Euronext Securities Copenhagen, Finance Denmark, e-nettet and Danmarks Nationalbank. RGA aims to identify and manage risks and incidents due to interdependencies between the securities settlement systems, retail payment systems and Kronos2. RGA works with, among other things, common shutdown and reopening scenarios as well as roadmaps and tests for controlled shutdown of the critical infrastructure in the event of operational incidents. The risk work in RGA and FSOR is coordinated on an ongoing basis.

**FSOR has identified 41 operational risks with the potential to threaten financial stability, and the members work together to mitigate the key risks.**

## FSOR puts strategic focus on data protection and recovery

As mentioned, the risk analysis identified several risks that involve data protection and recovery. This led FSOR to shift its focus to these areas.

One of the key initiatives is to identify data that is critical to society. Going forward, the work must be based on knowledge of the data that, from a social perspective, requires special protection, and what data to focus on in a recovery situation. In 2021, FSOR-RISK and RGA began work on jointly identifying critical data, including establishing a common understanding of what data is critical to society and developing a common model for classifying data.

Furthermore, data protection and recovery were taken into account in the design of the Baseline tool, which is described further below. FSOR also mapped the few existing community data protection and recovery solutions available in other countries to inspire further work. In addition, a workshop on data protection was held. Finally, Danmarks Nationalbank included data protection as a focus area in the forthcoming TIBER tests (*link*).

## Baseline tool will increase cyber maturity of the sector

In 2020, FSOR launched a project with the aim of developing a socalled Baseline tool based on the conclusions of the risk analysis.

Baseline will formulate specific and measurable recommendations for the work on cyber resilience in various areas, such as data protection or governance, in accordance with the existing legislation and established international standards. Baseline will be an IT platform in which each organisation can 'measure' its current cyber resilience on a voluntary basis and receive specified concrete actions which can be taken to achieve a desired level. Baseline can be used by all players in the financial sector and their suppliers. In 2021, the working group that is designing Baseline worked intensively to finish the tool, which was launched in early 2022.

## Survey of cyber resilience shows higher degree of resilience in 2020 than in 2018

In 2020, Danmarks Nationalbank conducted the third questionnai-rebased survey on cyber resilience among FSOR members. The study is a selfassessment of the current level of cyber resilience.

The results have been shared with each organisation to provide them with insights into where their organisation is compared to the other players in the financial sector. In addition, the overall results were discussed at an FSOR meeting.

The results of the survey are also used as input to the FSOR risk analysis and thus contribute to FSOR's decisions on what joint initiatives should be taken to address the most significant cyber risks in the sector.

In addition, based on the survey, FSOR held two best practice workshops on data protection and detection, respectively. The players who are best in class in each of these areas shared knowledge and experiences with the rest of the FSOR members.

In September 2021, Danmarks Nationalbank published the article 'How cyber resilient is the Danish financial sector?' (*link*) with an overview of the results of the survey on an aggregate level.

In the analysis, Danmarks Nationalbank assesses that the financial sector as a whole is strong in terms of its ability to protect systems and networks and detect external attacks – and stronger now than in 2018. At the same time, the cyber threat is rising primarily from ransomware attacks , and the techniques and tactics used by cybercriminals are constantly becoming more and more specialised and sophisticated. The risk that sophisticated hacker groups will breach external defences cannot be eliminated. It is important that the development of the threat landscape is continuously countered by appropriate security measures, including with a special focus on the work with data protection and secure recovery after a cyberattack.

**The best member organization with regard to data protection and detection have shared their knowledge and experience.**

## The crisis management team ensures coordination across the sector in the event of a crisis

Despite the good preventive measures, operational incidents will occur. FSOR has therefore prepared a detailed crisis management plan to ensure coordinated action across the financial sector in the event of a systemic crisis. It complements the members' own crisis plans and the national crisis response, NOST.

FSOR's crisis management was tested twice in 2021 to ensure that the plan works in practice in the event of a serious incident in the sector. On 15 June 2021, a partial test of the FSOR crisis management plan was carried out with the aim of practising an unannounced activation of the FSOR crisis management. On 23 November 2021, the FSOR Crisis Management Team carried out a test with special focus on the phases of the crisis management plan that aim to limit damage, remove the attack, restore business activities and deactivate the crisis response. In 2021, crisis management tests, among other things, led to updates to the FSOR crisis management plan, which is now available in version 4.0.

As in 2020, the pandemic also led to periods of lockdown and more working from home in 2021. During the period, the financial sector has not been operationally challenged in relation to being able to handle the functions that are critical to society.

## Round of visits to gauge temperature of FSOR collaboration

In 2021, the FSOR Secretariat visited the operational FSOR members. The purpose was partly to discuss the collaboration in FSOR, and partly to talk about the next steps in relation to the work on protection of the sector's critical data. Input from the visits indicates that the collaboration provides value across the sector, and that the members trust each other and have a common understanding. The input also provides an opportunity to align future resource expectations.

FSOR holds two annual member meetings, which serve as a forum for discussions and decisionmaking. Working groups are set up to develop and produce specific FSOR initiatives. Three working groups have currently been set up under FSOR, and a fourth is underway. Furthermore, ad hoc theme meetings are held with the aim of sharing knowledge in specific areas. In 2021, three theme

meetings were held on data protection, detection and the threat landscape, respectively.

## Cyber collaboration and continued focus on increasing resilience in 2022

Cyber resilience is high on the agenda throughout society
In addition to the initiatives launched in the financial sector under the auspices of FSOR, efforts are being made in society in general to increase cyber resilience.

At the end of 2021, the government announced a new national strategy for cyber and information security, covering the period 2022-2024. The strategy is an extension of the previous strategy for 2018-2021 and has as its ambition to strengthen digital security across society through 34 initiatives. The initiatives build on already implemented initiatives and also introduce new ones (*link*). It is expanded, among other things, from only covering the six current sectors that are critical to society to also include a wider circle of ministerial remits responsible for functions important to society.

For each of the sectors, a decentralised unit for cyber and information security, DCIS, has been established, as well as a sector strategy for the work. The Danish Financial Supervisory Authority undertakes the function as DCIS for the financial sector and is the lead on the financial sector's cyber strategy, which includes several of FSOR's abovementioned measures. The financial sector's cyber strategy expired in 2021, and a new sector strategy is expected to be launched in the first half of 2022 based on the new national strategy.

**Nordic cyber collaboration**
Annual cyber conferences are held among the Nordic countries. Players from the financial sector and authorities participate in these conferences, which aim to increase knowledge about cyber security across the Nordic financial sector. In November 2021, Norges Bank hosted the fourth conference with the theme 'Cyber security in complex value chains' (*link*). Here, the focus was on cyber risks in relation to suppliers.

In 2022, the conference will be held by the Central Bank of Iceland, Seðlabanki.

**International collaboration – CIISI-EU**
In 2021, Danmarks Nationalbank participated in all meetings in a publicprivate partnership between the most important European

financial players known as the Euro Cyber Resilience Board, ECRB (*link*).

The ECRB, which was set up after a decision made by the ECB decision in 2017, adopted a socalled 'Cyber Information and Intelligence Sharing Initiative (CIISI-EU)' in the beginning of 2020, under which a common platform has been established for knowledge sharing at strategic, tactical and operational levels between the major financial players in the EU (*link*).

Danmarks Nationalbank is a formal member of CIISI-EU and contributes, among other things, with experience from FSOR, which in relation to collaboration and sector initiatives is one of the frontrunners in an international context. Conversely, Danmarks Nationalbank regularly receives operational information and reports via CIISI-EU, which are used to enrich the current threat landscape and handle pending cases. During 2022, the focus will be on how this information can be exchanged to benefit more people, including how information from this forum can contribute to FSOR's other work streams.

**TIBER programme focuses on data protection**

Since the beginning of 2019, Danmarks Nationalbank has coordinated testing of cyber resilience in the financial sector under a programme called TIBER-DK. A special unit at Danmarks Nationalbank supports these tests and facilitates knowledgesharing among the participants of the programme. A TIBER test simulates advanced attacks from organised criminal cyber groups or statesponsored groups in real production environments. Based on intelligencebased threat information, the tests build on important tactics, techniques and procedures. The goal is to identify strengths and weaknesses of the cyber defence. Addressing the vulnerabilities increases cyber resilience.

Based on its positive experience with TIBER-DK, Danmarks Nationalbank and the individual participants decided in spring 2021 to continue the tests in future.

In future TIBER tests, Danmarks Nationalbank aims to have an added focus on data protection with a view to increasing efforts in this area. Therefore, all tests in the next round will as a general rule include an attack scenario with a special focus on data protection. The scenario can provide input on whether it is possible to gain access to reading, modifying or deleting sensitive data, whether it is detected when sensitive data leaves the organisation, and whether it is possible to access backup data in the event of an attack. In addition, work is being done to develop separate and more targeted tests of key, critical suppliers in the financial infrastructure.

The tests continue to follow the TIBER-DK framework, which in 2021 was updated with input from the TIBER participants and the ECB on the basis of the lessons learned so far with TIBER. The update accommodates the new focus on data protection and gives participants an even stronger learning base. Finally, at the end of 2021, the annual threat landscape report was prepared for use in the TIBER tests. The report was prepared by NFCERT with the involvement of relevant parties.

## New website to be published in 2022

In 2021, the FSOR Secretariat updated the FSOR website. The new website is expected to be launched in early 2022 with the aim of making it easier to access information about FSOR.