FSOR
FINANSIELT SEKTORFORUM
FOR OPERATIONEL ROBUSTHED

# ANNUAL REPORT 2017

In 2017, the Financial Sector forum for Operational Resilience, FSOR, celebrated its first anniversary. I am pleased that we – together with the financial sector – have continued our efforts to increase cyber resilience in the financial sector. This is necessary, if we are to realise the FSOR's vision that by 2020 the Danish financial sector should be "best in class in Europe when it comes to meeting the threat from cybercrime".

The cyberthreat did not diminish in 2017 – far from it. We have seen a number of cyberattacks hitting companies all over the world, and the costs of the attacks have been considerable. Danish industry heavyweights were also hit, highlighting that Denmark is no exception.

For this reason, we continued the work we started in 2016 and launched a number of new initiatives in 2017. For example, we conducted another test of the crisis response plans we put in place in 2016. And we have been working intensively to agree on the framework for a Danish "intelligence-led red team test programme". We managed to reach an agreement, so the Danish financial sector, like the financial sectors in the UK and the Netherlands, will be among the first to implement the programme and later to conduct such red team tests. To support the work of the FSOR, Danmarks Nationalbank took the initiative to hold the first joint Nordic cyber conference in 2017. The main purpose was to provide a forum for knowledge sharing on cyber resilience in the Nordic financial sector. You can read more about all that in this report.

One of the things that I am concerned about is how we at the FSOR can increase the involvement of and cooperation with non-financial sector players. The financial sector cannot be regarded as a desert island, and most of the issues we are dealing with at the FSOR are also relevant to other critical sectors and firms in Denmark. On the other hand, the management of cyber risk in other sectors could ultimately also affect cybersecurity in the financial sector. At the same time, the FSOR has received a number of requests from firms that would like to know more about the work of the FSOR. I think we should be open to that, and in 2018, Danmarks Nationalbank will consequently launch initiatives that could lead to more parties benefiting from the work of the FSOR and vice versa.

I am extremely satisfied with the FSOR's work in 2017 and would like to thank the participants in the FSOR for their dedicated effort. I look forward to continuing to work with you in 2018.

*Karsten Biltoft – Assistant Governor, Danmarks Nationalbank, and Chairman of the FSOR*

**FSOR participants** Box 1

- Banks and mortgage banks: Danske Bank, DLR Kredit, Jyske Bank, Nordea, Nykredit, Sydbank, Spar Nord
- Payment and settlement systems: Nets, VP Securities
- Data centres: Bankdata, BEC, JN Data, SDC
- Industry associations: Finance Denmark, Insurance and Pension Denmark
- Authorities: Centre for Cyber Security, Ministry of Business, Industry and Financial Affairs, Danish Financial Supervisory Authority, Danmarks Nationalbank
- Others: e-nettet, Financial Stability Company, Nasdaq

Danmarks Nationalbank chairs the FSOR and provides secretariat services.

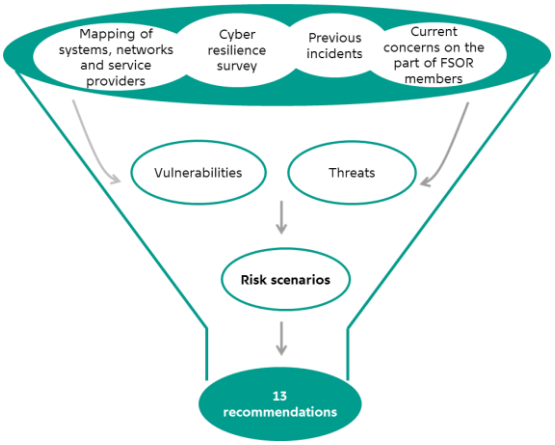
## RISK AND MAPPING

In 2016, the FSOR initiated comprehensive mapping of the most critical business activities, processes, systems and financial sector participants. This mapping was completed in 2017. It helps shed light on the interdependencies between participants in the financial infrastructure and has formed the basis for a risk analysis of the infrastructure.

The risk analysis points out the scenarios that are deemed to constitute the largest operational risks across the Danish financial infrastructure. The scenarios are based on an analysis of potential vulnerabilities and threats and includes e.g. the FSOR members' statements about current concerns and the results of the cyber resilience survey from 2016. This – confidential – risk analysis resulted in 13 specific recommendations, and the work to follow up on the recommendations is now well underway.

**Risk analysis results in 13 recommendations for the further work of the FSOR**

Chart 1




## TESTING OF CRISIS RESPONSE PLANS

In 2016, the FSOR 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 testing of the crisis response plans in 2016 led to various adjustments that were implemented in the spring of 2017. The second test of the response plans was conducted in the autumn of 2017. The test was a desktop exercise simulating several serious cyberattacks on key elements of the financial infrastructure. The main purpose of the test was to find out whether the participants, using the updated crisis response plans, were able to address the simulated attacks through cross-sector collaboration and response coordination. Once again, the test was managed by a recognised consultancy firm presenting its observations and recommendations for further strengthening of the FSOR crisis response. Against that backdrop, the FSOR will continue to strengthen its crisis response.

## RED TEAM TEST PROGRAMME

In 2017, the FSOR worked towards agreement on the framework for a Danish intelligence-led red team test programme for the financial sector. Agreement has now been reached. But a lot of work still remains to be done in terms of establishing the framework on which the red team tests are to be based. The first red team tests are expected to be carried outin  2019.

A red team test programme means a framework setting out common requirements for the testing process that each programme participant must complete. The framework ensures that all key financial sector participants are subject to a uniform minimum level of cyber

testing requirements and are tested for core functions. A simulated cyberattack on systems in production, i.e. live testing, is carried out for each programme participant.

The ECB is also developing a framework for implementing intelligence-led red team tests with a view to ensuring consistency and increasing the quality of the framework across countries. This is a major advantage to the Danish financial sector, since a number of large Danish banks have cross-border activities and could benefit from a consistent framework. Consequently, the ECB framework will also be the point of departure for a Danish programme.[1]

Finally, the work of the ECB serves to emphasise that if the FSOR is to fulfil its ambition to be best in class, Denmark must be among the first to use the ECB framework as a basis for setting up a red team test programme for the Danish financial sector.

**Quotation: Governor Lars Rohde on establishing an intelligence-led red team test programme for the Danish financial sector at Finance Denmark's annual meeting in December 2017**

Box 2

"... and we will also establish a so-called "intelligence-led red team testing programme" for the financial sector. I think this programme will be useful for the individual participants and for the sector overall. I also see it as a necessary step towards realising our vision of being best in class."

## 1ST ANNUAL NORDIC CYBER CONFERENCE

In 2017, Danmarks Nationalbank took the initiative to hold the 1st Annual Nordic Cyber Conference.

The main purpose of the conference was to support one of the key areas of action for the FSOR: knowledge sharing. Knowledge sharing on cyber resilience is essential in the fight against cybercrime.
The conference was arranged in cooperation with the other Nordic central banks. The financial sectors of the Nordic countries are comparable, and the largest financial sector participants operate throughout the Nordic region. Hence, a Nordic perspective is appropriate.

The conference was held in Copenhagen in the autumn of 2017 with 190 participants from the Nordic financial sector. The focus of the conference was on four main areas: the current cyberthreat scenario, how governments should respond to the cyberthreat, testing cybersecurity and, finally, the issue of cybersecurity regulation.

The conference was well received and has paved the way for even better knowledge sharing on cyber issues in the Nordic financial sector. At the conference, Finland announced that they will hold the next cyber conference in 2018.

Watch a few impressions from the event here: http://www.nationalbanken.dk/da/finansielstabilitet/fsor/Sider/1st-Annual-Nordic-Cyber-Conference.aspx

1 Read more about the ECB strategy for the work on cyber resilience in the publication "Cybercrime: from fiction to reality" from June 2017 (link).