FSOR

FINANCIAL SECTOR FORUM
FOR OPERATIONAL RESILIENCE

3 MARCH 2017

Annual Report 2016

In the spring of 2016, Danmarks Nationalbank initiated the establishment of the Financial Sector forum for Operational Resilience, FSOR.

The objective of the FSOR is to increase operational resilience in the financial sector, including resilience to cyberattacks. The participants in the FSOR are the key players in the financial sector, see box.

The Danish financial sector is one of the most digitised sectors in the world. That is a good thing, but it also means that the Danish banks and mortgage banks are closely interconnected via payment and settlement systems handling large values. Moreover, several financial institutions use the same data centres, network service providers, etc., so it is important that all key links in the chain are resilient and capable of resisting and managing operational incidents, including cyberattacks. In short, the FSOR has been established to ensure such operational resilience.

Two FSOR meetings were held in 2016. One of the results that I want to highlight is the "Vision for the cyber security of the financial sector" that we have formulated under the auspices of the FSOR, i.e. that by 2020 the Danish financial sector should be "best in class in Europe when it comes to meeting the threat from cybercrime". The vision was presented at the annual meeting of Finance Denmark1 on 5 December 2016 and contains a number of initiatives that we are

1 When the annual meeting was held Finance Denmark was called Danish Bankers Association.

to implement in the coming years. This requires a dedicated effort by all parties involved.

In 2016, we set up crisis response plans to ensure an efficient and coordinated cross-sector effort in the event of a critical operational disruption such as an extensive cyberattack, and we have also conducted a cyber stress test of the crisis response plans. And, finally, we have conducted a survey of cyber resilience in the financial sector. You can read more about this below.

The FSOR has made a good start. Everyone has made a dedicated and constructive effort. I would like to take this opportunity to thank the FSOR participants for that. Given the tasks ahead, we have to maintain the momentum. I am sure we can do that. I look forward to continuing to work with you in 2017.

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

FSOR Participants

Banks and mortgage banks
Danske Bank, DLR Kredit, Jyske Bank, Nordea, Nykredit, Sydbank

Payment and settlement systems
Nets, VP Securities

Data centers
Bankdata, BEC, JN Data, SDC

Industry associations
Finance Denmark, Danish Insurance Association

Authorities
Center for Cyber Security, Ministry of Industry, Business and Financial Affairs, Danish Financial Supervisory Authority, Danmarks Nationalbank

Others
e-nettet, Finansiel Stabilitet A/S, Nasdaq

Danmarks Nationalbank holds the chairmanship and provides secretariat for FSOR.

Vision for the cyber security of the financial sector

On 5 December 2016, the FSOR published a 2020 vision for the cyber security of the financial sector. The vision is an important indicator for the FSOR's future work. The level of ambition is determined by specific objectives and measuring points that the work of the FSOR must support and achieve.

The vision is that by 2020 the Danish financial sector should be best in class in Europe when it comes to meeting the threat from cybercrime. This would continue to provide a secure and efficient infrastructure and support the Danes' continued trust in the digital solutions of the financial sector. In order to measure whether the vision is realised, the FSOR has set up a preliminary proposal for measuring points:

1. Denmark is in the top 5 in international benchmarks for cyber security among financial firms in Europe.
2. Danish citizens and firms continue to have great trust in the sector's digital solutions.
3. The sector's losses as a result of cybercrime are in the bottom 5 in Europe.

The vision also formulates three main areas of action with associated activities:

- Strengthened collaboration within the sector and improved scope for action for individual sector participants.
- Stronger collaboration with relevant stakeholders both nationally and internationally.
- Increased awareness and knowledge of cyber security.

A key initiative of the vision is to ensure a shared overview of risks that could pose a threat to the resilience of the financial infrastructure. The increased digitisation is supported by complex IT systems and digital procedures that are linked across the sector. Due to the increasing complexity, detailed mapping of interdependencies between the systems and between the players is necessary in order to analyse whether the infrastructure contains vulnerabilities that need to be addressed.

In 2016, the FSOR consequently initiated a comprehensive mapping of the most critical business activities, processes, systems and financial sector participants. The purpose of this mapping is to help shed light on the interdependencies between sector participants and ultimately form the basis for an actual risk assessment of the overall infrastructure.

"Interconnectedness and the resultant interdependence between virtually all sector participants mean that knowledge-sharing and collaboration are essential if we are to stem the tide of attacks that will undoubtedly come in the future"

Governor Lars Rohde, at the annual meeting of Finance Denmark

Testing of the 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 the crisis. The crisis response plans expand the crisis communication plans that were established in 2008.

The new crisis response plans were tested in November 2016, since it is widely agreed in the FSOR that no matter how good the crisis response plans are in theory, they will only prove their worth in practice when they are tested and exposed to stress. The test, which lasted two days and was managed by a recognised consultancy firm, was a desktop exercise simulating several cyberattacks on key elements of the financial infrastructure. The purpose was to find out whether the participants in the crisis response were capable of addressing the attacks through cross-sector collaboration and response coordination.

The consultants prepared a report including observations, conclusions and recommendations.

Main conclusion of the report

”Our conclusion is that the sector test conducted fully and successfully tested the newly established crisis response plans, including the activation and capability of the response to manage a critical cyberattack. In our opinion, the test had great learning value for the crisis response group, and it pointed out a number of management, organisational and practical improvements that could strengthen the capability of the crisis response plans to efficiently manage an actual cyberattack in the future. Moreover, our assessment is that the crisis response secretariat generally functioned satisfactorily and worked professionally with the support of a highly cooperative and professional crisis response group.”

All in all, it was an instructive test that will be followed up by a new test in 2017 and more tests in the coming years. Link

Cyber resilience in the Danish financial sector

In 2016, Danmarks Nationalbank and the Danish Financial Supervisory Authority conducted a questionnaire survey in order to provide a picture of cyber resilience in the Danish financial sector. 15 key financial sector participants, who are also FSOR members, participated in the questionnaire survey.

Main conclusion of the survey

”The key financial sector participants in Denmark have strong focus on cyber security, but there is room for improvement.”

One significant observation from the survey was thatthe 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 employees alike. These participants also have a higher level of cyber security in several areas.

Furthermore the survey showed that with some participants there are room for improvement in the following areas:

- 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.
- All employees should be trained in cyber security, with special focus on employees with key business functions and access. The organisation could therefore benefit from giving those employees additional cyber security training.
- It would be useful to test crisis response plans against cyber incidents, as these may have special characteristics compared to other operational incidents.

Link