ANNUAL REPORT 2018

2018 was an eventful year for the Financial Sector forum for Operational Resilience, FSOR. And in my view, it culminated on 18 December, when Danmarks Nationalbank – as one of the very first in Europe – published the TIBER-DK (Threat Intelligence Based Ethical Red teaming) implementation guide. In the coming years, TIBER-DK is to ensure that the most critical financial institutions in Denmark participate in an ambitious red team test programme to increase their cyber resilience.

Danmarks Nationalbank is the authority of the TIBER-DK programme. Agreement to set up the programme was reached by the FSOR in February 2018. This very much reflected the value of the good cooperation with the sector that has existed since the establishment of the FSOR in 2016. The FSOR participants all agreed that if Denmark is to achieve the FSOR vision to be best in class, Denmark must have a TIBER programme.

We have also continued our efforts to increase cyber resilience in other areas. This applies both in relation to improving and developing the FSOR crisis response and in relation to following up on the recommendations of the 2017 analysis on cross-sector operational risks in the Danish financial infrastructure.

In 2018, we renewed our focus on knowledge sharing. This was reflected e.g. in a popular workshop following a cyber resilience survey conducted by Danmarks Nationalbank during the year. And in the autumn of 2018, our colleagues in the Bank of Finland held a Nordic cyber conference to follow up on the cyber conference initiated by Danmarks Nationalbank in 2017.

In the annual report for 2017, I emphasised that one of my ambitions for 2018 was to increase the involvement of and cooperation with players both inside and outside the financial sector. We are well on the way to meeting that objective.

As a new SIFI, Spar Nord has become a member of the FSOR, and for the cyber resilience workshop we increased the number of invitees to include firms with close links to the financial sector. We have also taken the first steps towards closer cooperation with the critical suppliers that we identified in connection with the analysis on cross-sector operational risks.

Last, but not least, at the end of 2018 we decided – jointly with the Danish Insurance Association – that the insurance and pension sector should become a more integral part of the FSOR in future, thereby allowing the FSOR to include the entire financial sector to an even higher degree.

The world around us is not standing still. In 2018, the cyberthreat did not diminish – far from it. In the spring of 2018, the central government launched an ambitious national cyber strategy and identified six critical sectors in that context, naturally including the financial sector, in which special efforts are to be made to increase cyber resilience. I fully agree with these ambitions, and Danmarks Nationalbank is prepared to continue the good cooperation, both in the FSOR and across the critical sectors.

Finally, I would like to take this opportunity to thank the FSOR participants for their constructive contributions to the FSOR agendas. Although the FSOR has existed for three years, I detect a continuing desire to share knowledge and to increase cyber resilience in the sector based on the conviction that greater cyber resilience will benefit all.

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

TIBER-DK

In February 2018, the FSOR agreed in principle to establish a Danish intelligence-based red team test programme. During the rest of 2018, a working group then worked to adapt the European TIBER-EU framework to Danish conditions. The adaptation resulted in a Danish framework called TIBER-DK, which was published by Danmarks Nationalbank in December 2018. This publication also marked the beginning of the testing process with the first tests taking place in 2019 and the remaining tests following in the course of 2020 and 2021.

TIBER stands for Threat Intelligence-Based Ethical Red teaming, and the programme was developed by the European Central Bank. TIBER sets a new pan-European standard for testing cyber security in the parts of the financial sector that are critical to society.

The test programme is intelligence-led, meaning that the test scenarios are based on intelligence on current and specific threats against the Danish financial sector and specifically against the individual test participants. In this way, the programme ensures realistic tests where test participants gain experience in defending themselves against the methods and tactics applied by real threat actors.

Coordination among authorities across national borders is an integral part of the TIBER framework. Cross-sector cooperation is an advantage as several test participants are operating in the Nordic region, and several Nordic countries are producing their own versions of the TIBER programme.

Together with the Belgian sector, the Danish sector will be the first to use the fully developed TIBER programme, and it will support the FSOR vision to become best in class in Europe when it comes to meeting the threat from cybercrime. Read more here:

http://www.nationalbanken.dk/en/financialstability/Operational/Pages/TIBER-DK-and-implementation-guide.aspx

CROSS-SECTOR RISKS

In 2018, work continued to follow up on the 13 recommendations from 2017 resulting from the FSOR analysis of cross-sector operational risks in the Danish financial infrastructure. For example, ongoing and formalised cooperation has been established to manage the risks arising out of the interaction between the core systems in the infrastructure, or which may affect several systems at the same time. Furthermore, risks related to the use of common critical networks and key service providers have been addressed, and the first steps have been taken to establish a common dialogue with the critical suppliers on how to jointly increase infrastructure resilience.

An analysis has also been performed to determine whether the precautions taken to detect and prevent criminal transactions are adequate. The aim of this work is to reduce the risk that IT criminals will be able to transfer large amounts in kroner out of the financial system, as seen e.g. in Bangladesh in 2016, when criminal managed to transfer 100 million US dollars out of the country.

THE FSOR CRISIS RESPONSE

Maintaining and developing the FSOR crisis response is a top priority. Therefore, efforts are ongoing to optimise the response. In 2018, a special focus area was to implement the improvements prompted by the crisis response test in 2017. In addition to that, focus was also on the choice of communication tools that can contribute to smoother communication in a crisis situation.

The FSOR also presented a detailed test plan for the coming years, which will contribute to the continuous enhancement and development of the crisis response.

SURVEY OF CYBER RESILIENCE

In the spring of 2018, Danmarks Nationalbank and the Danish Financial Supervisory Authority conducted a questionnaire survey of the cyber resilience of 16 key financial sector participants.

According to the survey, most participants assess that they have raised their levels of cyber resilience since the first survey in 2016. Most respondents indicated that they now have a cyber strategy that has been approved by the board of directors. This is a positive development as the survey shows 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 survey also showed that there is room for improvement. Few participants have not raised their levels since the 2016 survey, and they should give higher priority to their cyber security efforts. For the other participants, there also remains room for improvement in some areas. For instance, most of them can be more systematic and thorough in their efforts to ensure cyber resilience. At the same time, the capacity of cybercriminals is constantly growing. This means that a continuous effort is required to maintain a high level of cyber resilience.

The overall conclusions of the survey have been published (link), and Danmarks Nationalbank has provided individual feedback for the individual participants' further work to increase cyber resilience. A best practice workshop has also been held where participants that were best in class in various areas shared their experience.