Cyber security in the financial sector

VISION 2020

The Danish financial sector should be best in class in Europe when it comes to countering the threat from cybercrime, so that it:

- continues to provide a secure and efficient infrastructure, and
- supports the Danes’ continued trust in the digital solutions of the Danish financial sector.

We will increase awareness and knowledge of cyber security

We will strengthen collaboration within the sector and ensure improved scope for action for individual sector participants

We will strengthen collaboration with relevant stakeholders both nationally and internationally
All over the world, the IT systems of the financial sector and other critical sectors in society are attacked by criminals and by government-sponsored actors. Denmark is one of the most digitised societies in the world. Combined with the large values handled, this makes the Danish financial sector a target of cybercrime. The Centre for Cyber Security assesses the risk of cybercrime against Danish authorities and private sector firms to be very high.

The cyber threat is increasing
In 2016, there has been a tendency for IT criminals to target the business sector in Denmark. Most recently, in the PwC Cybercrime Survey 2016 PwC documented that 69 per cent of the respondent firms in Denmark had been hit by cyberattacks within the last financial year. CEO fraud is a new type of attack that is becoming more prevalent. In the first half of the year, Danish banks registered at least 92 successful attacks against Danish firms, resulting in total losses of more than kr. 60 million.

In some cases, the amounts involved are very large. In April 2016, the Danish prosecution service referred to two cases in which fraudsters had tricked Danish firms into transferring amounts of kr. 100 and 40 million, respectively. The use of ransomware, which means that IT criminals encrypt their victims’ computers and then require a ransom for decrypting them, has also increased strongly. A recent analysis by Trend Micro shows that at the international level, the number of ransomware attacks grew by almost 200 per cent in the 1st half of 2016 compared with 2015. Finally, the incidence of phishing and smishing has been rising lately, and consequently the Danish Bankers Association has decided to include this type of crime in its statistics of online bank hackings from 2016 onwards.

The methods used by IT criminals are constantly changing and becoming more and more sophisticated. In 2016, IT criminals succeeded in using the SWIFT infrastructure to rob the central bank of Bangladesh of 81 million dollars. The SWIFT system itself was not compromised, but insufficient IT security in the Bangladeshi central bank’s system made it possible for IT criminals to gain unauthorised access and use the SWIFT system for their criminal transaction. This gives cause for serious concern and is a topical example of how vulnerable our interconnected systems are.

Cyberattacks are a potential threat to financial stability
The financial sector depends on complex IT systems in order to function, and at the same time banks and mortgage banks are linked across the sector via data centres and payment and settlement systems. A
stable financial system relies, inter alia, on trust that book-entries of transactions are correct and are kept confidential, that settlement of payments and securities trades takes place in a timely manner and that customer-oriented systems are safe and accessible. Although the individual attacks do not as such have any impact on society, repeated cyberattacks on financial sector firms and systems may weaken confidence in the financial system. And an extensive cyberattack that compromises critical systems could potentially affect the whole sector or significant parts of it for a while. Hence, cyberattacks on the financial system are a potential threat to financial stability.

The individual financial sector participants have strong focus on IT security, including on making their systems resilient to cyber threats. However, the interconnectedness of the financial sector means that there is a need for a concerted and coordinated effort to counter the rise in cybercrime. Danmarks Nationalbank put this issue on the agenda of the Systemic Risk Council in December 2015, and at follow-up discussions with the financial sector there was broad agreement that it would be expedient to establish formal sector collaboration in this area. Against that background, the FSOR, Financial Sector forum for Operational Resilience was set up. The FSOR held its first meeting in June 2016.

**Financial Sector forum for Operational Resilience**
The FSOR is a forum for collaboration between authorities and key financial sector participants aiming to increase operational resilience when using IT across the sector, including resilience to cyberattacks. The tasks of the FSOR are to:

- Ensure a common overview of operational risks that may have a cross-sector impact and that could potentially pose a threat to financial stability in Denmark.

- Decide on and ensure implementation of joint measures to ensure financial sector resilience to major operational incidents, including cyberattacks.

- Create a framework for collaboration and information-sharing.

At present, the FSOR works along four tracks: establishment of national cross-sector crisis response for the financial sector, conducting a Danish cyber stress test, mapping and risk-assessing the financial infrastructure, and general stocktaking of the cyber resilience capability of key participants in relation to cyberattacks. The work of the FSOR addresses operational resilience in general, but with special focus on cyber resilience.

The FSOR finds that the above measures are obvious, appropriate and a good start, but also finds that there is a need to formulate a shared vision for the countermeasures to be taken by the financial sector against the increase in cybercrime.

This vision should encapsulate and align FSOR initiatives and the resultant measures to be taken by the individual banks and mortgage banks, data centres and payment and settlement systems.
Vision for the cyber security of the financial sector

The Danish financial sector should be best in class in Europe when it comes to countering the threat from cybercrime, so that it:

- continues to provide a secure and efficient infrastructure, and
- supports the Danes’ continued trust in the digital solutions of the Danish financial sector.

It is essential that financial sector customers have trust in the sector and in the digital solutions it uses. This is a precondition for realising the growth and innovation potential that lies in the digitisation of society.

Measuring points

In order to measure whether the vision is realised, three measuring points will be set up for the vision period, with attached indicators. The measuring points suggested are:

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.

These indicators are currently being clarified.
# Areas of action

To realise the vision, initiatives must be implemented within three main areas:

<table>
<thead>
<tr>
<th>Area of Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Strengthened collaboration within the sector and improved scope for action for individual sector participants</strong></td>
<td>The FSOR should create the framework for strengthened collaboration within the sector and improve the sector’s scope for action in relation to cyber threats and IT security threats. We want to be best in class in Europe when it comes to optimising and testing operational resilience capability across the sector. Stronger sector collaboration should also contribute to improving the individual participants’ ability to address cyber threats and IT security threats.</td>
</tr>
<tr>
<td><strong>Stronger collaboration with relevant stakeholders both nationally and internationally</strong></td>
<td>The FSOR should strengthen collaboration with relevant stakeholders, both nationally and internationally, with a view to sharing experience and best practice for countering cybercrime. This should improve the scope for specific action for FSOR members and for other stakeholders.</td>
</tr>
<tr>
<td><strong>Increased awareness and knowledge of cyber security</strong></td>
<td>The FSOR should help to ensure that all financial sector participants have the necessary knowledge and skills so that they will be able to protect themselves against cyber threats and IT security threats. At the same time, the FSOR’s work should contribute to improving the individual participants’ efforts to increase customer awareness and competencies as regards cyber security.</td>
</tr>
</tbody>
</table>
Initiatives in the coming years

Key initiatives in 2016 and the coming years are described below.

2016

In 2016, the primary focus has been on the aim of strengthening collaboration and the scope for action within the sector.

- Establishment of cross-sector crisis response to manage serious operational incidents, including cyberattacks.
- Conducting a cyber stress test of the cross-sector crisis response plans.
- Identification of critical participants and core functionality.
- Mapping of the infrastructure and interdependencies between the various participants.
- Stocktaking of key participants’ cyber resilience to cyberattacks.
- Investigation by FSOR participants of the possibilities of setting up a Nordic financial CSIRT.

2017-20

- Identification and assessment of operational risks that may have a cross-sector impact and could potentially pose a threat to financial stability.
- Preparation of a plan of action based on, inter alia, FSOR activities from 2016, including:
  - Initiatives resulting from the risk assessment.
  - Initiatives resulting from the stocktaking.
  - Initiatives to follow up the cyber stress test.
- Regular testing of the cross-sector crisis response plans with a view to improving/further developing these plans.
- Incorporation of relevant IOSCO recommendations on cyber security in the administration of the Danish payment and settlement systems.
- Ensuring coordination between the FSOR’s work and a forthcoming updated national cyber security strategy.
- Setting up collaboration with relevant FSOR counterparts in other countries.
- Setting up collaboration with a future Nordic financial CSIRT.
- Investigating the possibilities of intensifying collaboration with Nordic financial supervisory authorities, central banks and authorities responsible for cyber security.
Increased awareness and knowledge of cyber security

- Identifying international best practice for cyber security.
- Creating a framework for inviting international expertise to Denmark.
- Sharing knowledge about measures taken in various parts of the sector in relation to citizens’ and firms’ knowledge of IT security and ability to protect themselves better against cybercrime.

FSOR participants

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

Payment and settlement systems
Nets, VP Securities

Data centres
Bankdata, BEC, JN Data, SDC

Industry associations
Danish Bankers Association, Danish Insurance Association, Association of Danish Mortgage Banks

Authorities
Centre for Cyber Security, Ministry of Business, Danish Financial Supervisory Authority, Danmarks Nationalbank

Others
e-nettet, the Financial Stability Company, Nasdaq

Danmarks Nationalbank chairs and acts as secretariat of the FSOR.