SPEECH

SPEECH BY GOVERNOR LARS ROHDE AT THE ANNUAL MEETING OF THE DANISH BANKERS ASSOCIATION

DANMARKS NATIONALBANK

5 December 2016

CHECK AGAINST DELIVERY

Thank you for inviting me to speak.

I have these two key messages today:

1. Increased digitisation is good news for customers, banks and society in general.
2. Increased digitisation also makes the sector more vulnerable to destructive hacker attacks, but Danmarks Nationalbank and the sector are continuously working to prevent this.

***

The Danes have gone digital – and very much so. There are more mobile phones than people in Denmark, and nearly all homes are online. In fact, digital readiness is higher in Denmark than anywhere else. [Chart 1]

Technological advances have changed the way banks operate.

New possibilities have paved the way for a number of initiatives that have made the financial sector more efficient. This benefits the sector, and it benefits the Danes.

With increased digitisation, more processes can be automated and customers can increasingly serve themselves. This reduces the need for branches and employees – a trend that has been seen for some years as this chart shows. [Chart 2]

Technology has made digitisation a competitive parameter, which means that all banks are trying to attract customers by offering the best digital products.

However, it has also opened the door to increased competition from new actors, who will be able to enter areas that used to be completely dominated by the banks.

Competition is good, and there are no indications that we will have less competition in future. In fact, we can expect fiercer competition as a result of the EU's new Payment Services Directive, PSD2, which could be a game changer for the financial sector.

PSD2 allows third parties – with the customer's consent – to gain direct access to perform transactions in a customer's bank account. A third party could be e.g. a coffee chain, an airline company or another bank than the one where the customer has a deposit account.

The point is that PSD2 allows new actors to offer payment services without providing deposit accounts. Once they have got a foot in the door, they will also be able to offer other services, such as loans, which are actually sources of income for the banks – unlike payment services.

The Danish banks have been good at moving with the times and developing their own digital products. Examples are mobile payment solutions, which have become very popular among the Danes. These solutions have helped to prevent foreign actors from gaining significant market shares in Denmark until now. Obviously the limited size of the Danish market also plays a role.

Increased digitisation makes heavy demands on the individual banks if they are to keep up with technological advances and remain competitive. That is expensive. Typically it requires substantial investment, and in this respect the size of the bank is a factor.

The large banks are better positioned to develop their own digital solutions. Conversely, the small banks rely on collaboration with e.g. a data centre or a larger bank in order to be able to offer the solutions requested by customers.

Digital developments may increase the spread between small and large banks, as the large banks can typically benefit from economies of scale. So increased digitisation will contribute further to the downward trend in the number of banks. [Chart 3]

***

Increased digitisation also involves a degree of vulnerability. The financial sector relies on complex IT systems. Every day, nearly kr. 600 billion is transferred between accounts via those systems. That is equivalent to more than one quarter of Denmark's gross domestic product. And that makes the Danish financial sector an obvious target of cybercrime.

So today we are facing other threats than previously. There are still people like the Olsen Gang [Chart 4], but modern-day threats are radically different and may affect society as a whole.

In a historical perspective, cybercrime is a new type of crime, which can be committed from Herning, Hong Kong or anywhere else. We have already witnessed many attacks on financial institutions around the world. The attack on the Bangladeshi central bank made global headlines and was a warning that cyberattacks are becoming increasingly sophisticated.

The threat could well be even greater if it comes from organised hacktivism, terrorism or actual state-sponsored attacks.

An extensive attack that affects several critical actors or systems in e.g. the payments infrastructure could potentially paralyse the whole sector or significant parts of it for a while. Hence, unauthorised access to financial sector computers could constitute a systemic risk and ultimately threaten financial stability.

Even less serious attacks can – if they occur repeatedly – weaken confidence in the financial system.

This would be particularly critical if it were to happen at a time when the sector is already struggling – as it was in the autumn of 2008, for example.

That is the systemic angle which makes the cyber threat an issue for Danmarks Nationalbank.

One of the reasons why there is a systemic risk is that the Danish banks and mortgage banks are closely interconnected via payment and settlement systems handling large values. Moreover, the financial institutions use the same data centres, network service providers, etc. Consequently, it is important that all key links in the chain are very strong.

The Danish Financial Supervisory Authority and Danmarks Nationalbank have examined the cyber resilience of 15 of the largest and most important financial sector participants.

Although a survey of this type is subject to certain caveats, our conclusion is that, overall, cyber resilience is at a reasonable level – but there is room for improvement.

The risk of unauthorised access to or sabotage of important IT systems calls for IT security measures that perhaps received little attention previously.

Traditionally focus has been on severed cables, power outages or software errors. We still need to take these factors into account, but cybercrime poses new questions and requires new answers.

It is important to remember that attacks to computer systems are not unintentional. There are criminal minds at work, and they are constantly fine-tuning their methods. So the threats are changing all the time. This means that an attack may actually be difficult to detect in time.

Our survey shows that the individual sector participants are working with these challenges, but it also shows that the highest levels of security and protection against cyberattacks have generally been achieved by organisations with a cyber strategy which has been approved by the board of directors.

In other words, a strategy laid down by top management has helped to ensure focus on these issues throughout the organisation and to target efforts.

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

First and foremost, I would like to emphasise that collaboration is necessary – especially in situations where there is a potential threat to financial stability.

That is why we have established the FSOR – the Financial Sector forum for Operational Resilience.

The FSOR is a forum for collaboration between authorities and all key financial sector participants [Chart 5]. Its task is to implement "joint measures to ensure financial sector resilience". The focus is on preventing failures, but also on handling them if they, nevertheless, occur.

The ambitious vision for this collaboration is that we should be best in class in Europe when it comes to counter the threat from cybercrime.

The first specific initiative was the large-scale test of the financial sector's crisis response plans conducted the week before last. It really put the sector's ability to work together and coordinate efforts in the event of an extensive cyberattack on critical systems to the test.

It was an educational experience. We all learned a few lessons and came home with knowledge that we can use in our further efforts. And fortunately it was only a test. But if it becomes necessary, we are ready. It is better to activate the crisis response one time too many than one time too few.

One of Danmarks Nationalbank's tasks is to ensure that the Danish economy is robust. An important element of a robust economy is a financial sector with a robust infrastructure.

There is more work to do for the whole sector, but focus must be on the efforts made by the individual sector participants.

Thank you for your attention.