Andreas Dombret: A regulator's perspective on cyber resilience – how a management board can make a difference

Speech by Dr Andreas Dombret, Member of the Executive Board of the Deutsche Bundesbank, at the Cybersecurity Conference "Building a Safe and Resilient Digital Economy – Success Factors for an Agile Cyber Security Management", Munich, 11 February 2016.

* * *

1. Introduction

Dear Minister Aigner, dear Ambassador Ischinger, dear Mr Schlebusch,

ladies and gentlemen,

Thank you for inviting me to speak here today. Please let me start off on a note of optimism. The presence at this conference of so many well-known representatives from the corporate and political worlds demonstrates that we have already reached an important milestone on the road to cyber resilience: cyber risks are now receiving the attention they deserve.

This is not self-evident. Almost from the outset, it has been a struggle to draw the appropriate attention to cyber risk awareness, because it was widely assumed that IT is something for specialists, or simply an internal support factor for the company. If at all, managers spent more effort on discovering new IT-based services. As a result, innovative business applications emerged like algorithm-based credit-scoring, robo-advice or digital payment services, among others. Cyber risks remained largely unnoticed. In the meantime, several severe incidents such as the Stuxnet attack on Iranian nuclear sites, the intrusion into the German Bundestag network, and the penetration of cyber defences in around one hundred banks by the so-called Carbanak gang have helped to raise awareness of the issue.

Nowadays, cyber threats are no longer an abstract notion to us. We talk about criminal acts like "phishing" or "Trojan horse attacks". Whole strategies have become visible. Examples include "distributed denial of service" attacks – which means an overload of server requests or "man-in-the-middle" attacks, in which communications are secretly taped or even manipulated. According to a worldwide survey in 2015, 61 % of CEOs think that cyber risk is a key threat.[1]

You will not be surprised that the narrative doesn't end here. Awareness does not automatically imply appropriate understanding, and even then, conclusive steps on the path do not follow mechanically. To be specific, today, in many places cyber security has a name tag and a budget. But I agree with the results of many surveys and statistics according to which truly widespread cyber resilience is still a myth. In my speech today I want to outline – from my experience as a banking supervisor and as a central banker – how a management board taking the lead in this field can make a difference.

2. Cyber risk may cause real damage

Most of us, myself included, are not able to understand the source code of the online banking platform or firewall we are using. But for improving the cyber resilience of our economy, this information is not vital for us. Technical details can be translated into a more influential and more familiar language: namely, that of management and strategy. I come to this conclusion not from an IT specialist's perspective but instead from my experience in supervising one of the sectors of the German economy most vulnerable to cyber risks: the financial sector.

[1] http://www.pwc.com/gx/en/ceo-survey/2015/assets/pwc-18th-annual-global-ceo-survey-jan-2015.pdf.

In 2014, financial institutions were the leading purchasers of cyber insurance with average liability limits of US$57 million, followed by power and utilities firms and communications, media, and technology companies.[2] The fact that the financial sector is heavily exposed to cyber risks should be of no surprise. Obviously, the digitalisation of banking has led to a shift in the economics of financial crimes. Vast values are now stored on bank servers and no longer as cash in safes, and hacking is becoming an increasingly lucrative venture.

There are three independent ways in which a cyber attack may harm an entity or a person. In the financial sector, very often all of them are possible. Let's go through each of these breaches. (i) An integrity breach refers to manipulation of correct data. For example, during the Carbanak attack on banks, the thieves were able to mimic the staff and manipulate processes. They then instructed ATMs to dispense large amounts of cash. (ii) The theft of personal information is referred to as a confidentiality breach; in one prominent case of a US bank, over 60 million data records of private customers and companies were compromised. (iii) An availability breach represents yet another dimension of vulnerability. For example, criminals have frequently shut down online banking services, ATMs or other infrastructure powered by servers. Last but not least, cyber attacks may even ruin a bank's precious but non-digital asset: its reputation. In 2014, rumours about a bank being illiquid were distributed through emails and social networks – and out of this, an actual bank run happened.

In conclusion, the financial sector is not only a major target but is also vulnerable to almost every conceivable type of cyber risk. Pity for the financial sector, but good for the other industries because this makes it a repository of best practices which are also applicable to other parts of the economy.

My fellow banking supervisors at the Bundesbank and I have gained insights into cyber incidents, risk cultures and institutional preparedness across financial institutions. We are witnessing growing concerns about cyber risks, not only nationally but also on a European scale and as part of the international financial stability community.

But you should not be surprised that the Bundesbank is also a target of cyber attacks: As a central bank, we provide critical infrastructure for the banking system and for payment services, and therefore we are a potential target ourselves. All of this together helps us to accumulate knowledge about the status quo and developments in cyber defence in the financial sector.

3. What have we learned?

Let me share with you what I think might be some important lessons we have learned thus far.

First, there is no free lunch in the cyber world. We are able to make thousands of transactions in a second and transmit huge amounts of data across the globe at the click of a mouse, but at the same time we are exposed to the risk of high-speed and high-volume losses. There is a trade-off for every innovation. But before you can assess the trade-off, you have to know what elements are being traded off against each other. For example, at the Bundesbank, we have identified a trade-off between the need to use mobile devices and the need to use data sparingly; we now ask our staff to use mobile data only when necessary.

Second, there simply is no such thing as 100% cyber security. As a measure of defence, two-factor authentication is considered as best practice for online banking applications. Not because it is undefeatable – but because it seems to be a sound compromise between customer convenience and IT security; it requires only a little additional effort on the part of

[2] Figure refers to cyber liability total limits purchased by companies with revenue of $1 billion or more. Source: Marsh (2015) – Benchmarking Trends: As cyber concerns broaden, insurance purchases rise. Available online [most recently accessed on 8 February 2016] at: http://usa.marsh.com/Portals/9/Documents/Benchmarking-TrendsCyber8094.pdf.

customers, yet at the same time the additional layer of security imposes a higher hurdle for cyber criminals to clear authentication.

Third, defending from cyber risks is by no means trivial, but requires a considerable degree of foresight and ingenuity. Threats are constantly evolving. In order to control and mitigate cyber risk, banks are even starting to use big data to discover unusual patterns that point to a cyber attack. From a governance point of view, setting the right priorities can make a huge difference. We have seen cases in which banks expend a lot of resources on deterring sophisticated assaults while omitting the most basic of measures. I am especially referring to a factor which is still highly underappreciated: the human factor. For humans are often the weakest link in IT processes. Targeting "digital carelessness" among customers and staff is usually a good way to achieve fast results in mitigating risk.

4. How to cope with cyber risks

These insights have been incorporated into regulatory and supervisory practice. Unsurprisingly, regulation cannot give a detailed prescription for cyber security, because the cyber environment is so agile that technical details can quickly become obsolete. In addition, there is no one-size-fits-all solution that can cover the diversity of the types and sizes of institutions.

There are, of course, concrete elements for cyber defence that would not be out of place on a checklist for any institution: network plans with appropriate security layers, contingency and recovery plans and a well-conceived update management, to name some important items.

But indeed, there is more to cyber resilience than a functional first line of defence. It requires responses to new as well as unknown circumstances that at the same time maintain the functional viability of an institution. This gives senior management a lot of room for manoeuvre. The tone from the top is instrumental in raising staff awareness of security issues. Also, companies and organisations are evolving constantly. Managing responsibilities is thus key. This includes breaking down the "accountability firewall", where nobody assumes responsibility for the many intersecting aspects of cyber risk. We therefore demand that banks clarify what is at stake and how the risks are supposed to be governed. This is called a cyber strategy, and every bank is required to have a convincing one.

In summary, we do not expect bank CEOs to understand each and every technical detail – but it is the overall responsibility of the management board to manage the risks in an adequate way. They need to have a concrete idea of what is at stake. This might be an unavoidable obligation for executives, but at the same time investing appropriately in cyber security will frequently pay off handsomely.

5. Beyond sector limits

Ladies and gentlemen, the internet has become one of our constant companions – by the same token, cyber defence must become one as well. As I said earlier, actual resilience requires deliberate action in each company from the top down. Let me reiterate a few key tasks for senior management:

> Recognise cyber risks as part of your risk appetite and define a convincing and comprehensive cyber strategy
>
> Ensure that responsibilities remain clear in a changing cyber and corporate environment
>
> Raise awareness among your staff and set an example in promoting secure cyber behaviour

A holistic cyber defence will not emerge bottom-up from your IT department – you need to lead towards it. This applies to all industries, but also very much to the financial sector.

I have omitted one success factor so far. One that transcends sector limits. I am referring to cooperation for mutual learning. To quote an old proverb: Wise men learn by other men's mistakes; fools by their own. We can benefit a lot from others' experience across industries and national boundaries. The Bundesbank is a member of UP-KRITIS, a platform for providers of critical infrastructure to exchange ideas and information. We have also launched international exchange on cyber defence, for example with the Federal Reserve Bank of New York. Merging defence capacities is a good reason for voluntary collaboration. Still, I detect resistance in some institutions, partly because of the delicate issues involved, and partly because of a lack of trust and out of reputational concerns. However we should try to find ways to overcome those barriers – with cyber criminals collaborating globally, our success might depend on us following suit.

Thank you.