Joachim Wuermeling: Cybersecurity - pivotal for central banks

Keynote speech by Prof Joachim Wuermeling, Member of the Executive Board of the Deutsche Bundesbank, at the 2nd Payments Drift Forum, Euroforum, Aschaffenburg, 7 September 2017.

* * *

1. Introduction

Ladies and gentlemen

Thank you for the opportunity to speak to you today. The Payments Drift Forum is a wonderful platform for practitioners, politicians and officials.

I highly appreciate the opportunity to address this group and to contribute to what looks like a very interesting and comprehensive two days of dialogue around current developments in the field of payments and banking operations.

In his keynote address, Winfried Bausback just talked about an issue that is – and will continue to be – extremely relevant for the industry: cybercrime. Let me use this opportunity to weigh in and address the issue of cyber security from a central banker's standpoint.

2. There is no such thing as "absolute security"

When it comes to information technology there is no such thing as absolute security. The security expert Gene Spafford hit the nail on the head when he said, "The only truly secure system is one that is powered off, cast in a block of concrete and sealed in a lead-lined room with armed guards".

Just think of the incident at the central bank of Bangladesh. In February 2016, 81 million US dollars was misappropriated, and the shock among all financial market players was painfully clear. This is understandable; after all, the last German report on the protection of the Constitution stated that cyberattacks bring annual losses of around €55 billion to the German economy. The cost to the global economy is supposedly €400 billion. More than half the businesses in Germany (53%) have fallen prey to cyberattacks in the past two years. One in six businesses (17%) had sensitive digital data stolen during this period, with the attackers primarily getting their hands on e-mails (41%) or financial data (36%). These facts should be a reminder for German businesses to boost their cybersecurity.

It goes without saying that these facts are also spurring us at Bundesbank to ramp up our efforts in securing our own systems. Our infrastructure being up and running is not only crucial for us as an institution, but it's also critical for the financial system in Germany and the Euro area.

Let's look at TARGET2 for instance, a wholesale payment system operated by Deutsche Bundesbank, Banca d'Italia and Banque de France. More than 1,000 banks all over Europe are directly connected. The service ensures the speedy and final settlement of national and cross-border payments in central bank money. Each working day, an average of around 350,000 payments with a value of about 1.7 trillion Euro – which equals half the German GDP last year – are processed by the system. TARGET2 is just one example for critical financial market infrastructure for which Bundesbank is in charge. Others include TARGET2 Securities, a service for the settlement of securities in central bank money. Or think of our monetary policy operations, which provide the banking system with liquidity. A proper functioning of these services is crucial for the stability for our financial system.

But how does the Bundesbank interpret the term "cybersecurity"?

At the Bundesbank, we refer to cybersecurity when our focus is on protection against cybercrime and the associated risks.

We define cybercrime in the following ways.

- There is a deliberately targeted and IT-based attack on data and IT systems
  - which can viably impair confidentiality,
  - integrity, or
  - availability.
- Additionally, the unauthorised use of internet capabilities
  - to spread information very quickly,
  - in large volumes, and
  - on a broad scale.
- Finally, we understand cybercrime to include the procurement of personal information through social engineering.

In these ways, the attackers usually gain either broad reach or access to a specific target.

To what extent has the Bundesbank been hit by attacks?

Cyberattacks also pose a risk to the infrastructures and applications of European central banks, which is not to be underestimated. There are four reasons why central banks, in particular, are a lucrative target for cyber espionage and cyberattacks.

1. Because of their economic and policy mandate,
2. Because, as a result, information is available to them at an early stage,
3. Because of their responsibility for cash-based and cashless payment systems, and
4. Because of their prominent role in their country's financial system.

Last year, the Bundesbank was also the target of isolated distributed denial-of-service attacks. These involve known systems being overloaded by a flood of requests and thus brought to a standstill.

The Bundesbank has used its protective measures to successfully fend off the attacks aimed at it so far. Last year alone, we intercepted around 10,000 e-mails infected with malware and stopped a hundred thousand unauthorised attempts to access the Bundesbank infrastructure.

Possible reasons for broad reach

Cyberattacks like the one recently experienced by the central bank of Bangladesh show, on the one hand, how vulnerable all businesses are once an attacker can take control of the internal network. On the other hand, a clear trend is evident that financially motivated attackers have significantly enhanced their tactics, techniques and processes, making it harder to detect, analyse and remedy the attacks. In targeted attacks like these, it can often be months or years before anyone realises that their systems have been compromised and, in some cases, that data has secretly been siphoned out.

On 12 May 2017, WannaCry infected around 200,000 systems in 150 countries around the world, according to Europol. The malware encrypted all available network data. It was spread by

exploiting a vulnerability in the Windows operating system (EternalBlue), which was discovered by the NSA, and stolen and leaked by the hacker group Shadow Brokers.

More recently, attackers have also aimed to cause maximum damage within a short timeframe. The businesses hit by NonPetya weren't even able to react quickly enough because the damage was already done in a short space of time by wiping parts of the hard disk. The Danish container shipping company Maersk estimates the damage caused by the NonPetya attack at between 200 and 300 million US dollars, according to its own statements. These examples are further proof that businesses have to manage their cyber risks at least as scrupulously as they do their traditional risks.

While banks can offset the losses incurred by the default of an average borrower, just one successful cyberattack can bring the activities of a bank to a standstill, no doubt causing immense reputational damage in the process.

What's more, the financial sector is highly interconnected, meaning that the default of a single participant can lead to disturbances being felt throughout the entire industry. If, for instance, a stock exchange or payment system were to default, thousands of participants would be affected on the spot.

The financial sector is also an obvious target for politically motivated attackers. By hitting a critical infrastructure, attackers would be able to not only inflict direct financial damage but also wreak havoc on the economy at large.

For the financial sector, in particular, it is therefore becoming increasingly important to press ahead with measures in order to defend against cyber risk such as:

- Optimise centralised and decentralised protective measures on an ongoing basis.
- Foster a culture of cybersecurity.
- Bolster the resilience of financial market infrastructures.

3. Cybersecurity as a quantifiable metric is feasible

Looking at the examples that I have cited, it would be fitting to find that financial market participants were complying with a uniform security standard. But this is not the case.

What difference would such a "uniform security standard" make?

First of all, as we draw up our defensive measures, it is vital that we all borrow from established standards such as

- the international Code of practice for information security management (ISO/IEC 27002),
- the US NIST Cybersecurity Framework or
- the German IT Baseline Protection Catalogues of the Federal Office for Information Security.

Compliance with these standards is important and guarantees a middling level of protection. Generally speaking, however, attackers are not interested in firewalls – they are interested in their weak points. It is therefore important that enterprises identify their own vulnerabilities and rectify these using standardised procedures.

Let's take a look at the Top 20 Critical Security Controls. These standards were put together by a large number of government and industry experts in cybersecurity and represent a prioritised, risk-based recommendation for implementation. Such procedures would help us increase awareness of existing weaknesses. In addition, they would serve as a guideline for implementing effective processes and tools to appropriately secure our systems.

In this context,

- constant monitoring,
- automating processes,
- providing uniform evaluation metrics, and
- acquiring knowledge of real attacks

are all crucially important with respect to developing effective defence systems. This is what we can do, and I appeal enterprises to follow these procedures.

This is because we need to first reach a point where we can identify the current state of cybersecurity using established risk management procedures before going on to

1. find room for improvement and
2. continually improve quality standards ("majority level").

Effectively searching for and finding weak points is therefore one of our main tasks, especially since our capabilities in this regard pale in comparison to those of the attackers.

Liability for manufacturers

Besides the enterprise itself, what can others do? Just like Federal Minister of the Interior Thomas de Maizière and Arne Schönbohm from the Federal Office for Information Security, I expect manufacturers – no matter how short their products' life cycles are – to be required to

- identify bugs at an early stage,
- report them,
- close them as quickly as possible and
- make security updates available for a longer period of time.

The developers of hard- and software must be forced to adhere to IT security standards and to integrate and activate safety functions into their products. Such a legal obligation could have a great impact to the multitude of IT products that are subject to weaknesses. Therefore, in addition to the product-specific security requirements regarding product liability and product safety laws, the infringement of technical standards and rules – such as DIN standards, common criteria and protection profiles – should lead to a presumption of guaranty or the facilitation of the affected parties.

I myself am a big fan of "bug bounty" programmes, which are run by many international companies and offer financial rewards to ethical hackers (known as "white hats") for reporting bugs – and that's because vulnerabilities that we have been unaware of up to now are another problem that we need to address. Deutsche Bundesbank therefore supports manufacturers and suppliers conducting bug bounties. As the number of professional attackers grows – irrespective of whether they are cybercriminals or intelligence agencies – so too does the likelihood of their hacking tools becoming the target of attack. The Shadow Broker and Vault 7 documents released on WikiLeaks make these risks abundantly clear.

Penetration tests are helping

Penetration tests are an effective means of unearthing previously unknown vulnerabilities in systems and applications and then eliminating them. They clarify the extent to which attackers can penetrate an organisation's infrastructure and how much damage they can cause. A single weak point can be all it takes for attackers to hit the jackpot.

In my opinion, “red teaming” is the ultimate in penetrating testing. This involves a red team, usually brought in from outside, working against an internal team of analysts (the “blue team”) whose mission is to defend the internal infrastructure to the best of their ability. European financial market infrastructures are to be subjected to this manner of cyber testing with the aid of a standardised European red team testing framework. I would like to encourage you to regularly review the resilience of your own infrastructure and processes and to develop them successively.

In the Bundesbank, annually a large number of vulnerability checks and penetration tests take place. We detect and fix regularly weaknesses of the manufacturers or ourselves in systems and applications.

The weak link: people

Well-known hacker Kevin Mitnick – who allegedly hacked into the US Department of Defence’s network more than one hundred times and penetrated NSA systems on multiple occasions – once said: “Companies spend millions of dollars on firewalls, encryption, and secure access devices and it’s money wasted because none of these measures address the weakest link in the security chain: the people who use, administer, operate and account for computer systems that contain protected information.”

I agree with Kevin Mitnick. This stems from the fact that, in all of the cyberattacks known to us, attackers focused their attention on people as the weak link: in other words, end users and their behaviour. That is why I think it is essential to raise awareness among users about how to handle data and IT systems in a security-conscious manner – and this awareness needs to be conveyed to all those who work with such systems.

Each and every one of us must

- develop an understanding of the threats, yet
- internalise the fact that these threats are constantly changing and
- that it is possible to protect ourselves.

And this applies in both the work and the private setting. In the Bundesbank, we regularly discuss current threats, organize seminars focusing on cyber-security, or – like in the past year – perform a large-scale awareness campaign which dealt with subjects like “data classification", “encryption", “password protection", “mobility” and “social engineering".

This means that the analysis and synthesis of vulnerabilities are our tools of choice when it comes to heightening security awareness within the company and to giving management a deeper insight into the actual risk situation.

It would be desirable to establish a system of measures and metrics that renders visible the progress already made.

4. Is 99% security enough?

While banks can absorb the losses incurred by the default of an average borrower, just one successful cyberattack can bring the activities of a financial market infrastructure to a standstill, causing at least immense reputational damage or in the worst case a financial crisis.

The onus is therefore on banking supervisors to keep an even closer watch than they do now on the potential threats posed by cybercrime. And the central banks have a special responsibility to protect themselves from cyber risks, thereby safeguarding confidence in the financial system. That’s why we’re also working closely together at the international level to reduce cyber risks for ourselves and for the financial market infrastructures.

One example of this cooperation is the “Guidance on cyber resilience for financial market infrastructures", which was published in 2016. The Bundesbank, in cooperation with the Federal Financial Supervisory Authority (BaFin) as well as the central banks and the supervisory authorities of the other G10 countries, drew up requirements for financial market infrastructures with regard to cyber risks.

It is of fundamental importance that not only information technology plays its part. Everyone concerned must bear responsibility: the technical experts, every single user and the supervisors.

The global ransomware attacks have once again clearly demonstrated how vulnerable digital infrastructures are.

Last year, BaFin and the Bundesbank, along with representatives from banks and banking associations, discussed the supervisory requirements for information technology. These requirements were drawn up to encourage a more detailed examination of supervisory expectations on the technical and organisational resources specified in the Minimum requirements for risk management (MaRisk), to clarify them and to render them more transparent. Thoughts were fleshed out on the basis of the IT strategy in place in other areas such as access management, application development and the management of externally procured IT services.

Thus, protection against increasingly sophisticated IT threats is and remains a never-ending task. The level of IT security achieved therefore has to be constantly reappraised and improved – as it is true for every other criminal menace.

5. Cooperation and coordination are key

The examples I have just mentioned illustrate the ongoing potential for optimising the reliability and robustness of the hardware and software we use as well as the eradication of faults.

The systems that manage our reserve assets have a high level of IT security, and the necessary protective measures can be installed in near-real time. It was in this context that the Federal government and the Bundesbank made cybersecurity a focal point of Germany’s G20 presidency. And that is why we spoke about the issue of cybersecurity in great depth at the meeting of G7 finance ministers and central bank governors. This was where, in October 2016, the G7 Fundamental elements of cybersecurity for the financial sector were adopted. The G7 Cyber Expert Group is tasked with presenting the key aspects of an effective assessment of cybersecurity by October of this year.

Together with the cybersecurity experts of the other central banks we are, moreover, continuously monitoring the current global threat level and regularly consult with each other to initiate any countermeasures. And last but not least, we are constantly striving to optimise our detection and defence systems, as we take every attack that is launched against us very seriously.

We urgently encourage other institutions, too, to exchange their knowledge and to liaise with each other at the national and international level on their critical infrastructures.

6. Attack is the best form of defence

Ladies and gentlemen, attack is the best form of defence. At least, that’s what football pundits tell us. But our turf, the cyberworld, is a place of stealth and cunning, and this particular football adage doesn’t apply. Indeed, the opposite approach is called for: protect yourselves against attack and

- Make IT security your goal.

- Establish a company-wide security culture.
- Continue to adapt to the changing and ever-evolving threat situation.
- Seek out security vulnerabilities in your company.
- Optimise your risk management structure constantly.
- Keep contingency plans and competence rules at the ready in case of a crisis.
- Share information, thoughts and experience with each other.

And please, always bear in mind: IT security is not a product you can buy. It's a process that has to be embraced.

There's no such thing as absolute security, we are not immune to attacks. But it is our job to prepare to the best of our ability for possible threats.

Another word of wisdom, yet again from the world of football, is the following: Attack wins you games, defence wins you championships. So let's make sure our defence is in good shape.

Thank you for your attention.