BaFin Perspectives

Issue 1 | 2020

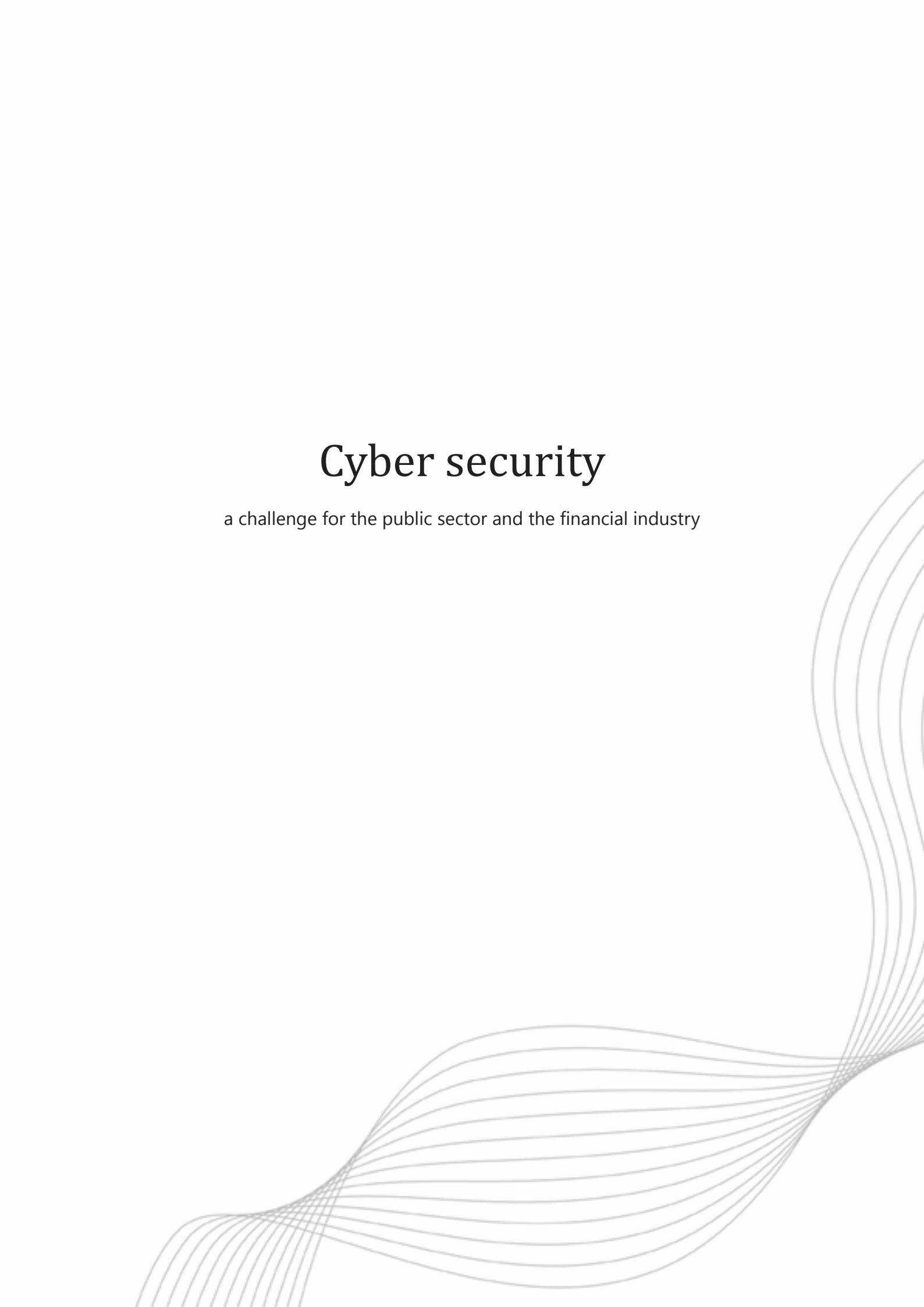
BaFin

Bundesamt für Sicherheit in der Informationstechnik

Cyber security

Cyber security

a challenge for the public sector and the financial industry



Contents


© iStock/in-future

Foreword

Millions in lost earnings, painful losses in productivity at financial institutions – even customer trust is ultimately on the line. Around the globe, cybercriminals are attacking the IT security systems of banks, insurers and other financial services providers in order to gain access to sensitive data, such as names, addresses, telephone numbers, passwords and account numbers. They insert malware into the IT systems of financial institutions to demand a ransom, threatening to bring entire IT systems to a standstill. Such scenarios have become commonplace, which is why the attention of all staff and appropriate IT security measures are needed.

In Germany alone, the overall economic losses caused by cybercrime have doubled to over EUR 100 billion in the last two years according to estimates provided by the digital association Bitkom. Cybercriminals have got their eye on the financial industry, and there are attacks on financial institutions almost on a daily basis.

Given the high level of professionalism among these cybercriminals, we believe that it is necessary to make room for a more in-depth discussion on this topic and to connect key players in the industry and the public sector. This is because trust and effective cooperation – from prevention right up to crisis management in the event of a cyber attack – is essential to allow Germany, as a financial centre, to become more resilient to cyber threats.

On behalf of the Federal Financial Supervisory Authority (BaFin) and the Federal Office for Information Security (BSI), we have

therefore decided to jointly publish this BaFinPerspectives issue, entitled "Cyber security – a challenge for the public sector and the financial industry". BaFin and the BSI have been working in close cooperation for many years. We regularly discuss IT security in the financial sector, share information on technology trends and standardisation, and assess current situations, too. Both of these federal authorities provide their expertise, allowing new information and insights to be taken into account in their joint work on critical infrastructures, covering banks, insurers and service providers, among others.

We hope you will find it interesting to read.

Felix Hufeld
President of BaFin

Arne Schönbohm
President of the BSI

I

Current threat landscape and discussion on effective measures

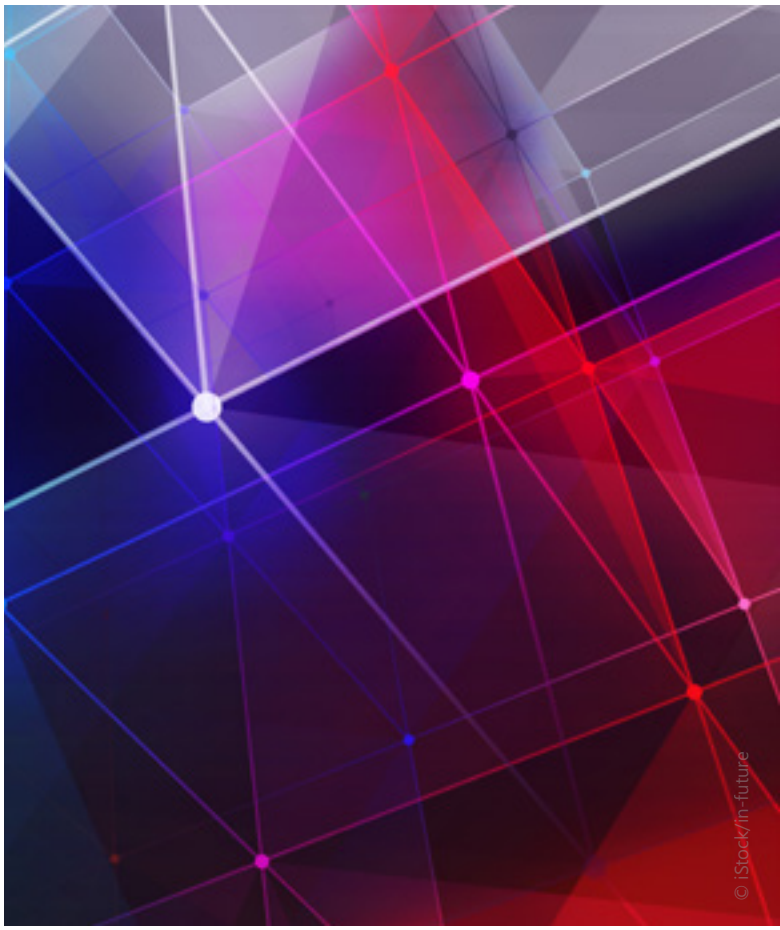
Digitally helpless? A brief survey of IT security in Germany

Author

Tim Griese
Deputy Press Spokesman, Federal Office for Information Security (*Bundesamt für Sicherheit in der Informationstechnik* – BSI)

1 Introduction

In what continues to be a critical IT security environment, the sophistication of many cyberattacks has increased.[1] A significant risk is posed to government, business and society by Emotet[2], which the Federal Office for Information Security (*Bundesamt für Sicherheit in der Informationstechnik* – BSI) described in December 2018 as the most dangerous malware in the world. This assessment was confirmed by the considerable damage that was inflicted again and again due to cyberattacks with Emotet during 2019. Those affected included numerous universities, hospitals, local authorities and companies, as well as private users. Financial service providers were also among the targets but, as far as the BSI is aware, were able to repel the attacks they suffered.



1 This article is based on the BSI report The State of IT Security in Germany in 2019. The report contains a comprehensive, well-founded survey of the current threat landscape in cyberspace: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Securitysituation/IT-Security-Situation-in-Germany-2019.pdf?__blob=publicationFile&v=3, last accessed 23 April 2020.

2 Emotet is a Trojan that, for example, extracts data from Outlook contacts and e-mails, and propagates malware by sending out spam mails disguised as replies to the genuine e-mails it has intercepted. Familiar subject lines and quotations from previous correspondence make the fake e-mails appear authentic to their recipients.

2 Types of threat

2.1 Ransomware

Apart from Emotet, ransomware too continues to be one of the greatest threats faced by companies, public authorities, other institutions and private users. Time and again, ransomware has disabled computers, networks and even production plants. Furthermore, public bodies were also targeted repeatedly by ransomware attacks during 2019, including hospitals and local administrations. One trend can be observed in this context: attacks are purposely being directed at central service providers, via which their customers or connected networks can be infected with ransomware. The potential damage is enormous: the costs inflicted by production downtime, losses of data, and the cleaning-up and restoration of systems can run into the millions, while public bodies may only be able to deliver their services to a limited extent, if at all.

2.2 Identity theft

The new sophistication in cyber attacks that had been predicted by the BSI was also apparent in a number of serious cases of identity theft that made the headlines in 2018 and 2019. The victims included users of social networks, the customers of major hotel chains and, as a result of a doxing incident that came to light in January 2019, hundreds of celebrities and politicians in Germany. Hundreds of millions more Internet users saw their data being made publicly available on the Internet by a series of data breaches known as "Collection #1" to "Collection #6", which offered easy pickings for other cybercriminals as well. What is remarkable about these incidents is not just their increasing frequency, but also the huge volumes of personal data leaked and subsequently posted on the Internet.

2.3 Botnets

The threat from botnets continues to remain grave. In this field too, attackers are exploiting digitalisation, and focussing on mobile end-user devices and Internet-of-things (IoT) systems. In 2019, up to 110,000 bot infections were registered every day on German systems, and reported by the BSI to the relevant network operators for decontamination. Even greater potential for attacks is offered by server-based botnets, particularly in light of the increasing use of cloud infrastructure. Over half of all attacks are executed with cloud servers that have been compromised or illegitimately rented. Accordingly, almost every cloud service provider has now been misused by criminals to execute DDoS[3] attacks on at least one occasion.

2.4 Malware

Attackers continue to display a great deal of ingenuity in (further) developing their malware and attack mechanisms. About 114 million new malware variants were identified from June 2018 to May 2019. The potential threat posed by malware spam continues to rise, even though the number of spam mails being sent has actually decreased. Nonetheless, e-mails containing malware are among the most frequently detected kinds of attack launched against the German Federal Administration. The impact of such malware is growing, not just in traditional office communication, but also in productive sectors of the economy.

What is, in any case, a critical cyber security environment is being exacerbated unnecessarily by users' frequent helplessness in relation to all things digital. Criminals deliberately exploit weaknesses in individuals' approaches to security, combined with products and systems that are not adequately protected at a structural level. The situation can be remedied by the systematic application of "state-of-the-art" IT security techniques, as well as by strengthening every single user's sense of "digital responsibility".

3 Distributed denial of service.

3 An integrated value chain protecting government, business and society

Even against the background of the alarming threat landscape, it is nonetheless possible for digitalisation to be managed securely. If Germany is to be an attractive place to do business and also maintain its security levels in the future, it will be necessary to seize the opportunities offered by digitalisation while, at the same time, countering the potential risks appropriately from the outset. As a hub for business and innovation, Germany must be a pioneer of digitalisation, ensuring that safeguards are built into IT products and corporate networks at their conception, and that the principles of security by default[4] and security by design[5] become second nature.

As the German Federation's competence centre for IT and cyber security, the BSI has been successfully doing the groundwork for this approach, and has shouldered much of the responsibility for putting it into practice, although it is a task that has to be embraced by the whole of society. Every day the BSI scrutinises the fields in which digitalisation is being applied where risks could arise, and how such risks can be rendered both calculable and controllable. Nearly 30 years experience of building up and bundling know-how in the cyber security field have made the BSI a highly competent agency that acts as a nerve centre for Germany's cyber security efforts. The BSI draws on the lessons it has learned over this period to make appropriate recommendations, and design products and services that meet the diverse requirements of government, business and society. Bringing together prevention, detection and response under one umbrella, this integrated cyber security value chain is one of the things that give the BSI its unique standing.

4 Security by default means that IT products and devices have to be secure when they are supplied. All security features must be preconfigured in such a way that the user has to adjust as few settings as possible themselves.

5 Security by design means that security is integrated into a product's development process as an explicit requirement and that, from project initialisation on, holistic security measures are taken into account, implemented, tested and technically certified before the product is rolled out.

“Cyber criminals are relatively lazy”

Interview with

Arne Schönbohm
President of the Federal Office for Information Security (BSI)

Felix Hufeld
President of the Federal Financial Supervisory Authority (BaFin)

Both Schönbohm and Hufeld admit that they have personally had trouble with hackers in the past. In an interview with BaFinPerspectives on the seventh floor of the BSI’s headquarters in Bonn, Arne Schönbohm and Felix Hufeld discussed a number of solutions to tackle the threats from cyber space.

Mr Hufeld, have you ever been the victim of a cyber attack?
Hufeld: Ten years ago, I received an e-mail on my personal laptop about an allegedly unpaid invoice. I was so outraged and, at the same time, inexperienced that I clicked on the link in the e-mail. Just like that, I was faced with a serious ransomware problem. My computer screen froze and I had to get it fixed by an IT specialist, which was pricey. It was all a real nuisance. But at least I didn’t pay a ransom. I’ve been more careful since.

Have you ever had a similar unpleasant surprise yourself, Mr Schönbohm?
Schönbohm: Yes, I was the victim of an IT security incident at the start of the year – although this wasn’t because of something I had done. A car rental company from which I had previously rented a car was hit by a cyber attack in early 2020. This attack led to the release of a large amount of personal data, including my personal e-mail address and telephone number. There was also information on who had been doing what where and how. I then received several phishing emails along the lines of “Dear Mr Schönbohm, we are updating your Sparkasse account details”. After taking a closer look at the sender, this turned out to be a scam.

How do you protect yourself from threats in cyber space?
Hufeld: I carefully check the e-mails I receive. This is highly effective, as simple as it seems. I regularly change my passwords, too. I also have an effective antivirus software installed on my personal computer to filter out most of the malware at least – this is something we do at work in any case. And yet some phishing e-mails still manage to make their way through. Only good instincts can help in such cases.

And what advice would Germany’s chief cyber security officer have to offer?
Schönbohm: It is true that there is always the risk that a cyber attack will be successful. Nobody is spared from this risk. It is therefore important to prepare crisis responses at an early stage in order to limit the damage as far as possible. Some advice I would give is to make extra copies of personal photos on an external hard-drive, for instance. In the event of a ransomware attack, the data would be quickly retrievable.

Data theft, extortion and sabotage: new cases of cyber crime are reported on a regular basis. Does the government have the tools to tackle such criminal activity?
Schönbohm: Yes, absolutely. We have successfully thwarted cyber attacks, which Germany's public administration is constantly exposed to as well. This is thanks to our good network infrastructure and the IT Security Act (*IT-Sicherheitsgesetz* – IT-SiG), which was adopted in 2015. But this is very much like the story of the tortoise and the hare.

Could you give an example?
Schönbohm: Cyber attacks involving widespread spam campaigns such as the Emotet malware or attacks targeting vulnerabilities in Citrix products were inconceivable just a few years ago.

How does Germany stand in comparison with other countries?
Schönbohm: We are in a good position in terms of information security. Germany has succeeded in establishing a centre of expertise in this area: the BSI. We are also setting an example by making the information at our disposal available to other key government institutions. In the area of finance, for instance, we are working closely with BaFin and the Bundesbank.

Which country serves as a role model for Germany?
Schönbohm: Germany closely follows what is being done in France, with its rather centralised structures. Both countries are in close contact. The approach taken in Israel is also particularly interesting.

Why?
Schönbohm: In Israel, the security forces – which includes the Israel Defense Forces, for instance – research and industry all work in close cooperation. Moreover, Japan is a strong player in terms of innovation. We are sharing information with many countries on a regular basis, as we want to learn from the very best.

According to the stereotype, the typical hacker wears a hoodie and sits in front of a computer in the dark. Does this stereotype hold true?
Schönbohm: These hackers certainly still exist, in TV shows or on streaming services, for instance. But in real life, there are also hackers who are involved in organised crime operating around the world.

What different kinds of hackers are there?
Schönbohm: There are hacktivists who want to make a political statement with a website defacement. If we look at the example of the Hambach Forest, which

has been the subject of protests in Germany for years now, hacktivists change, for instance, information on the website of an energy group with the intention to influence the debate. Other hackers will attack critical infrastructures simply out of anger. And there are those who target public sector institutions or large corporations in order to extort money from them with ransomware. Last but not least, there are hackers who have considerable technological skills and seek to obtain information with methods used by intelligence agencies.

Which areas are particularly vulnerable to attacks?
Schönbohm: All areas that you can make money with and that can be accessed easily. Cyber criminals are relatively lazy. Minimum effort, maximum reward: this is the principle they live by. This is why it is all the more important to ensure that the baseline protection measures set out by the BSI are fully implemented.

What overall economic losses are caused by cyber crime?
Schönbohm: According to estimates, the potential losses caused by cyber crime in Germany has doubled in the last two years, amounting to over EUR 100 billion. But how can such an amount be measured? Does this include the development costs for a new product? Lost profits? A missed opportunity on the stock market? Or system recovery costs after an attack? We need to develop a common understanding here.

The financial industry is attacked by cyber criminals at a rate like no other. What are the trends regarding the number of cases?
Hufeld: There has been a striking increase in DDoS attacks on financial institutions since the start of the year. Around 600 security incidents have been reported to BaFin over the last two years. And we can expect the number of cases to rise in the years to come. One thing is clear: the banks that were hit in the good old days will be the victims of attacks in a digital world as well.

What happened in these security incidents?
Hufeld: Most of the IT security incidents that were reported to us were not the result of external hacker attacks but were due to internal vulnerabilities at institutions. A series of unusual events can lead to significant damage and losses. I still have the impression that there is a certain tendency to underestimate internal vulnerabilities and the well-known "human factor" as the cause of IT security incidents.

Are you saying that staff members are to blame in most cases?
Hufeld: Criminally motivated external attacks are also on the rise. The drama that unfolds after an external attack has an explosive nature and draws more attention, too. In the meantime, people are happy to overlook many of the small mistakes that are made on a daily basis. This is a huge mistake in my view.

The banks, insurers and financial services providers that meet certain criteria are considered critical infrastructures. Why do cyber attacks pose such a high risk for these institutions in particular?
Hufeld: Financial transactions keep the real economy going. If anyone were to deliberately or inadvertently interfere with these transactions, they would not only block abstract cash flows but they would also interfere with the interrelations in the real economy that underlie these cash flows. This is a highly sensitive issue.

And what are the risks?
Hufeld: Highly sensitive and personal data concerning individuals or families that none of us want in the public sphere are stored. No one would want such data to be used to blackmail them. It is also worth mentioning something that is specific to the financial sector: cyber attacks do not just have an impact on individual banks, insurers or other financial institutions because they are all interconnected. As a result, these attacks can lead to systemic risks relatively easily, for example, through contagion channels that are extremely difficult to identify.

What are the consequences in such cases?
Hufeld: It could jeopardise the stability of the financial system as a whole. This is a matter of trust. When millions of people panic and we see the infamous queues in front of ATMs or bank counters, this is not necessarily caused by hard facts – rumours are enough. This can lead to incredible bottlenecks and waves of human behaviour. In some countries, this has had

systemic consequences. For this reason, the financial sector, as a critical infrastructure, needs to be protected in a particularly intelligent way.

A DDoS attack recently brought a direct bank's online banking services to a standstill for hours. Do institutions have enough expertise to protect themselves?
Hufeld: In theory, yes. But our experience in financial supervision has shown that there is still much room for improvement. Following recent events, I was alarmed to find out that even IT service providers, who, in their professional capacity, offer precisely these services on a daily basis, can be easily thrown off course by a relatively simple cyber attack. This was also revealed in most of the findings of BaFin's inspections at institutions. Although the industry has understood the magnitude of this challenge, a lot more still needs to be done. We are far from being able to rest on our laurels.

How do BaFin and the BSI respond to serious cyber attacks?
Schönbohm: There are staff-level exchanges between the BSI and BaFin to inform each other about what has happened exactly and to assess the situation. In these exchanges, we also set out the matter at hand and determine the type of support we can provide to the institution in question. Mobile Incident Response Teams can be taken as an example here.

Is this some kind of rapid reaction force?
Schönbohm: Yes. In most cases, the operations of a company's IT department are designed around IT systems that function properly in normal conditions. If a cyber attack occurs, this can have huge consequences, especially if the institution under attack has not prepared for such an event. This is why prevention is just as important as crisis response. Our experts help companies experiencing acute attacks by determining how operations can be up and running again. We also help them find a service provider to retrieve data and define the company's crisis communication.

How are BaFin's supervisors overseeing IT service providers that are operating in the financial sector?
Hufeld: The outsourcing of a wide range of IT services, with only a small portion being done in-house, is more the rule than the exception. This is perfectly fine, too. As financial supervisors, we ensure that certain quality and monitoring requirements are taken into consideration in outsourcing financial institutions in their agreements with service providers, for instance.

Does BaFin have direct access to these service providers?
Hufeld: The situation is currently heterogeneous. Interestingly, BaFin has traditionally had far-reaching access rights in the area of insurance supervision. We have fewer options in the area of banking supervision, though. There will need to be a discussion on how we should respond from a regulatory perspective to the increasing significance of outsourcing for the financial system as a whole. For instance, this could be done by expanding the traditional range of tools at our disposal under supervisory law. I definitely think such a discussion is necessary and it has already begun in international regulatory bodies.

Before the coronavirus crisis, cyber fraud was considered the top business risk for companies according to Allianz's 2020 Risk Barometer. Do you have the same impression based on your experience in financial supervision?
Hufeld: Yes, people are now generally aware of the threat situation. I believe only few bank executives haven't acknowledged that there are considerable risks in the area of IT. Information security is a top-level issue in risk management. After all, information security risks could threaten the existence of a financial institution in the worst case scenario.

Are financial executives acting accordingly?
Hufeld: I cannot say that this is being managed adequately day in day out. There is still a long way to go before a satisfactory level is achieved.

Companies are reluctant to publicly speak about cyber crime. Rightly so?
Schönbolm: No, this is the wrong strategy. When a cyber incident occurs at a financial institution, it is important that the incident is directly reported to the BSI or BaFin. All information is treated as confidential. The worst thing that could happen would be a company trying to hide the fact that they have been hit by an attack. Cyber criminals often proceed in a similar way and look for different victims in the same industry. If we are informed about an attack, we can also warn others at an early stage.

BaFin's financial supervisors regularly inspect the internal IT systems of institutions, even if an acute cyber attack hasn't occurred. Why?
Hufeld: Ensuring that the organisation of a business is able to run smoothly is essential for financial institutions to continue operating – this is similar to capital requirements and liquidity management, for instance. As you can imagine, the financial sector strongly depends on IT systems that work. This is why IT must be treated as a key component of all traditional monitoring and supervisory activities.

What is your approach?
Hufeld: As a financial supervisory authority, we started by clearly setting out what we expect from the institutions we supervise. We systematically developed our supervisory requirements for IT in financial institutions (BAIT), followed by similar requirements for the insurance industry (VAIT) and asset management companies (KAIT).

What else has been achieved?
Hufeld: We have significantly reinforced our ability to inspect IT security systems at institutions. We have developed specialised structures at BaFin for this purpose. This has now become an essential part of our supervisory and inspection activities. In addition, BaFin is increasingly testing the resilience of institutions. We are also currently implementing the TIBER-EU framework at national level. And we are making preparations should acute events occur at institutions.

There are also insurance policies to cover losses caused by cyber crime. How is cyber risk assessed?
Hufeld: Cyber risk is a relatively new phenomenon; as it is manifesting itself in different ways, it is also keeping insurers on their toes, and rightly so. When creating new products such as cyber insurance policies, insurers must observe a number of basic parameters that have existed for centuries. The scope of cover, reinsurance coverage, trigger events and the characteristics that are considered by insurers when determining premium rates are important when pricing a new risk.

Is it possible that cyber risks are lying dormant in older insurance policies?
Hufeld: I was indeed concerned that there would be risks hidden around in insurance policies. This is why BaFin examined, in close cooperation with the industry, whether such risks could be found in less recent insurance policies. Silent cyber risks can ultimately lead to major losses and damage if these risks materialise.

What were your findings?
Hufeld: Our suspicion was that cyber risk policies were not tariffed appropriately in some cases - e.g. because the insurer did not even have cyber risk on its radar in the coverage it provided many years ago. But it turned out there was hardly any reason for concern. I was relieved by the findings of our survey.

Online banking, digital payments and internal processes: digitalisation has given financial institutions the opportunity to change the structure of their business models. Is cyber crime limiting their ability to do so?
Hufeld: No, I do not think this will put an end to innovation. I am an optimist, which is why I believe in the innovative capabilities of people, politicians and the industry. We will find solutions, no matter how the digital transformation will unfold over the next few years. We are constantly having to weigh up the objectives of innovation, speed and convenience on the one hand and safety and security on the other. All the wonderful things we want to achieve must be done in a safe and secure environment – the challenge is to find the right balance between both sides of the spectrum. In light of the typical public policy choices to be made, it is our responsibility as authorities to suggest ideas to politicians on how to achieve different and yet perfectly legitimate political goals, all while finding a reasonable balance.

Mr Schönbohm, do you share this optimism?
Schönbohm: Yes, absolutely. I think that we are in a much better position in Germany than we sometimes think. For instance, Estonia is considered a shining example in the area of IT security, but this is ultimately based on German expertise, such as the BSI's IT baseline protection recommendations (*BSI IT-Grundschutz*).

Germany also has the most information security certifications in the high-security sector worldwide. As a nation and as a country of entrepreneurs, Germany is able to combine two strengths: its open-mindedness and its digital mindset. These are excellent conditions to successfully shape the digital transformation process, while achieving the right balance in terms of information security.

Mr Schönbohm, Mr Hufeld, thank you for your time.
Interview by Annkathrin Frind, BaFin Communications Directorate

Profile
Arne Schönbohm, President of the Federal Office for Information Security (*Bundesamt für Sicherheit in der Informationstechnik* – BSI)

About Arne Schönbohm: Schönbohm has been the BSI's President since 2016. Prior to this, he was President of the German Cyber Security Council (*Cyber-Sicherheitsrat e.V.*) and worked as an IT security consultant. Schönbohm studied international management in Dortmund, London and Taipei. He began his professional career at DaimlerChrysler Aerospace. He then held various management positions at EADS.

About the BSI: The BSI is the central IT security service provider for the German government and is subject to the oversight of the Federal Ministry of the Interior (*Bundesinnenministerium* – BMI). The authority, which is based in Bonn, is responsible for ensuring that the German government's networks are secure. It is also responsible for the protection of critical infrastructures.

Profile
Felix Hufeld, President of the Federal Financial Supervisory Authority (*Bundesanstalt für Finanzdienstleistungsaufsicht* – BaFin)

About Felix Hufeld: Hufeld has been BaFin's President since 2015. Prior to this, he was the Chief Executive Director for Insurance Supervision at BaFin. Hufeld, who is qualified in law, studied in Mainz, Freiburg and Harvard. He started his career at The Boston Consulting Group. He then worked at a number of companies, including Dresdner Bank and the insurance broker Marsh.

About BaFin: BaFin supervises banks, financial services providers, insurers and securities trading. It is an institution under public law and is subject to the legal and technical oversight of the Federal Ministry of Finance (*Bundesfinanzministerium* – BMF).

The supervision of information security and cloud computing needs to be harmonised across Europe

Authors

Silke Brüggemann
Senior Advisor, BaFin Division for Policy Issues relating to IT Supervision and Inspections

Sibel Kocatepe
Advisor, BaFin Division for Policy Issues relating to IT Supervision and Inspections

1 Introduction

The harmonisation and convergence of supervisory requirements for financial entities is the basis for a stable financial market and for strengthening the digital operational resilience of the financial sector. For this reason, the European Commission has shifted the focus towards this political project: With the FinTech action plan[1] (see info box, page 26), which has now been completed, it is seeking to create not only a more competitive and innovative – but also a more secure – European financial sector. The Commission has provided details on the measures it is considering in the areas of information security and cloud computing, which are key to achieving the aforementioned goal. This was part of its "Financial services – improving resilience against cyberattacks (new rules)" initiative[2] in December 2019.

In early April 2020, the European Commission also published its "Consultation on a new digital finance strategy for Europe/FinTech action plan"[3] to build on the FinTech action plan mentioned above. The findings of this public consultation, which will end on 26 June 2020, will be incorporated into a new five-year digital financial strategy/a new FinTech action plan. While the consultation published in December 2019 looked into digital operational resilience, this consultation seeks views on how to ensure that the financial services regulatory framework is technology-neutral and innovation-friendly while maintaining a cautious approach as regards consumer protection. Moreover, the consultation seeks views on how to remove fragmentation within the European Economic Area for digital financial services, and how best to promote a well-regulated data-driven financial sector. With the publication of this digital finance strategy/FinTech action plan, which is scheduled for the third

1 European Commission, FinTech action plan: For a more competitive and innovative European financial sector, https://ec.europa.eu/transparency/regdoc/rep/1/2018/EN/COM-2018-109-F1-EN-MAIN-PART-1.PDF, retrieved on 10 March 2020; see info box, page 26.

2 European Commission, Financial services – improving resilience against cyberattacks (new rules), https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12090-Digital-Operational-Resilience-of-Financial-Services-DORFS-Act, retrieved on 6 May 2020.

3 European Commission, Consultation on a new digital finance strategy for Europe/FinTech action plan, https://ec.europa.eu/info/consultations/finance-2020-digital-finance-strategy_de, retrieved on 21 April 2020.

quarter of 2020, the European Commission is seeking to address the challenges associated with the advancement of digitalisation and strengthen the innovativeness of the European financial sector.

In light of these developments, the present article offers an overview of the progress made to date as part of Germany's and Europe's efforts to harmonise requirements in the area of information security (incl. cyber security) and in the area of cloud outsourcing.

However, it should be noted that this article does not claim to be exhaustive. It is limited to information that has been made available to the public by supervisory authorities and European institutions in the financial sector. This article does not contain any non-disclosed information, or information on supervisory practices in particular, as this is confidential.

An overview of global regulations in the area of information security is provided in the info box below.

At a glance

International publications on information security requirements

A general overview of international regulations in this area can be found in the Financial Stability Board's (FSB) document entitled "Stocktake of Publicly Released Cybersecurity Regulations, Guidance and Supervisory Practices",[4] which was released in 2017.

The Basel Committee on Banking Supervision (BCBS) has also compiled a list of global practices in the banking sector in its 2018 publication entitled "Cyber-resilience: Range of practices".[5]

The International Association of Insurance Supervisors (IAIS) has provided a similar overview for the insurance sector, with its "Application Paper on Supervision of Insurer Cybersecurity"[6] (November 2018).

In the area of financial market infrastructures, the Cyber Task Force of the International Organization of Securities Commissions (IOSCO) offers a comparable analysis in its Final Report.[7]

4 FSB, Stocktake of Publicly Released Cybersecurity Regulations, Guidance and Supervisory Practices, https://www.fsb.org/wp-content/uploads/P131017-2.pdf, retrieved on 12 January 2020.

5 BIS, Cyber-resilience: range of practices, https://www.bis.org/bcbs/publ/d454.pdf, retrieved on 16 December 2019.

6 IAIS, Application Paper on Supervision of Insurer Cybersecurity, https://www.iaisweb.org/file/77763/application-paper-on-supervision-of-insurer-cybersecurity, retrieved on 12 January 2020.

7 IOSCO, Cyber Task Force – Final Report, https://www.iosco.org/library/pubdocs/pdf/IOSCOPD633.pdf, retrieved on 12 January 2020.

2 Harmonisation of regulatory requirements in Germany: BAIT, VAIT and KAIT

With the publication of its Supervisory Requirements for IT in Financial Institutions (*Bankaufsichtliche Anforderungen an die IT* – BAIT)[8] in 2017, its Supervisory Requirements for IT in Insurance Undertakings (*Versicherungsaufsichtliche Anforderungen an die IT* – VAIT)[9] in 2018 and its Supervisory Requirements for IT in Asset Management Companies (*Kapitalverwaltungsaufsichtliche Anforderungen an die IT* – KAIT)[10] in 2019, BaFin made it clear early on, in comparison to its international counterparts, how supervised financial entities are expected to ensure sound IT governance.

These three circulars are the cornerstone of information security supervision in Germany. With these circulars, BaFin has also addressed key shortcomings that were revealed during IT inspections at financial entities in recent years. The common objective is to create a clear and flexible framework for information security management, raise awareness in this regard throughout financial entities and provide transparency on how BaFin expects management boards to ensure appropriate information security – both within financial entities and in relation to third-party service providers.

Financial entities are obliged to ensure they have a sound governance system in place. The three circulars on supervisory requirements for information security are aimed at offering entities clarity and certainty on the requirements for IT strategy, IT governance, information risk management, information security management, and the outsourcing of services.

The circulars also cover technical aspects of information security, such as requirements for user access management, IT projects, application development and IT operations. However, they remain technology-neutral.[11]

Financial entities must implement the requirements on a principles basis, taking into account the principle of proportionality. Overall, BaFin follows a convergent and harmonised regulatory and supervisory approach. For this reason, Germany's financial supervisor uses the same terminology in all three circulars while also taking into account sector-specific aspects. Examples include references in the BAIT and KAIT to the corresponding minimum requirements for risk management at institutions (*Mindestanforderungen an das Risikomanagement* – MaRisk) or those applicable to asset management companies (*Mindestanforderungen an das Risikomanagement von Kapitalverwaltungsgesellschaften* – KAMaRisk). The sections on critical infrastructure (*KRITIS-Module*) in the BAIT and VAIT serve as another example.

8 See BaFinJournal January 2018 (only available in German) and BaFin Circular 10/2017 (BA) - Supervisory Requirements for IT in Financial Institutions (Bankaufsichtliche Anforderungen an die IT – BAIT), https://www.bafin.de/dok/10445406, retrieved on 6 May 2020.

9 See BaFinJournal April 2018 (only available in German), page 24 et seq. and BaFin Circular 10/2018 – Supervisory Requirements for IT in Insurance Undertakings (Versicherungsaufsichtliche Anforderungen an die IT – VAIT), https://www.bafin.de/dok/11721176, retrieved on 6 May 2020.

10 BaFin Circular 11/2019 (WA) – Supervisory Requirements for IT in Asset Management Companies (Kapitalverwaltungsaufsichtliche Anforderungen an die IT – KAIT) of 1 October 2019, https://www.bafin.de/dok/14116416, retrieved on 6 May 2020.

11 See BaFin's supervisory priorities for 2020, page 9, https://www.bafin.de/dok/13918786, retrieved on 6 May 2020.

3 Harmonisation of regulatory requirements for information security at financial entities in Europe

With the publication of the FinTech action plan[12] (see info box), the European Commission invited the three European Supervisory Authorities (ESAs) to develop joint proposals on how entities in the financial sector can strengthen and improve their cyber resilience (see info box).

At a glance

FinTech action plan

In March 2018, the European Commission published its FinTech action plan for a more competitive and innovative European financial sector. The objective was to help financial entities make better use of innovations driven by technology. Through the measures described in its action plan, the Commission aims to promote innovative business models and encourage financial entities to make use of new possibilities such as distributed ledger technologies and cloud services. Considerable focus is placed on the action plan's third measure and its primary goal: strengthening the cyber resilience of financial entities.

At a glance

Cyber resilience

The term "cyber resilience" describes an entity's ability to withstand attacks on the security of its information and communications technology (ICT). Attackers focus on company systems or even customer data.

12 loc. cit. (footnote 1).

In response to this, the European Insurance and Occupational Pensions Authority (EIOPA), the European Banking Authority (EBA) and the European Securities and Markets Authority (ESMA) published their "Joint Advice on the need for legislative improvements relating to Information and Communication Technology (ICT) risk management requirements" [13] in early April 2019. In this joint advice, the ESAs propose concrete measures to the European Commission for the harmonisation and convergence of requirements relating to information and communication technology (ICT) at financial entities.[14]

Where there is a need for harmonisation

The ESAs' joint advice shows where there is a need for harmonisation, taking the European insurance sector as one of several examples. Although 22 of the 28 EEA Member States had information security guidance and/or legislation in force when EIOPA conducted a survey in this regard, there are still apparent differences in terms of how legally binding the requirements are. These requirements are set out in a range of laws, circulars, guidelines, guidance or mixed forms of the above.

The vast majority of the legislation/guidance in place covers the main areas of information security, including IT strategy, IT risk and security management, IT operations and third party management. However, the level of detail and the aspects covered in the different requirements vary significantly.

On the other hand, the survey revealed that just over 50% of the legislation/guidance published in EEA Member States cover malware, patch management and

13 Joint Committee – European Supervisory Authorities, Joint Advice on the need for legislative improvements relating to Information and Communication Technology (ICT) risk management requirements – JC 2019 26, https://eiopa.europa.eu/Publications/JC%202019%2026%20(Joint%20ESAs%20Advice%20on%20ICT%20legislative%20improvements).pdf, retrieved on 10 March 2020.

14 See BaFinJournal April 2019 (only available in German), page 26 et seq.

anti-virus management, security awareness and training, and IT governance.

In sum, EIOPA's survey shows that there is a wide range of national regulatory requirements covering various areas with a different level of detail. In addition, the requirements vary in terms of how legally binding they are. In order to address this heterogeneity, EIOPA announced in the ESAs' joint advice that it would develop information security guidelines. In doing so, it is following the steps taken by the EBA, which launched a consultation on its draft guidelines at the end of 2018.[15] Although ESMA is not currently working on its own information security requirements, it is promoting information sharing among national competent authorities (NCAs) regarding cyber threats.[16]

Ultimately, the ESAs consider that it is necessary to harmonise and supplement information security requirements in all sectors. The ESAs believe that the harmonisation of requirements across the financial sector with regard to governance requirements will result in a higher overall security level, appropriate supervisory practices in the area of information security and an improvement in cyber security, for instance.

The ESAs hence called on the European Commission to supplement the relevant European Directives with information security aspects in order to create a common baseline across all financial sectors. The Commission referred to this proposal in its consultation document entitled "A potential initiative on the digital operational resilience in the area of financial services"[17], published in December 2019 as part of its "Financial services – improving resilience against cyberattacks (new rules)" initiative.[18] Using a questionnaire, the European Commission asked stakeholders in different areas about their views on the further harmonisation of information security requirements in order to increase digital operational resilience[19] in the financial sector. This process took place until mid-March 2020. The European Commission has not yet published the results of this consultation. The ESAs, on the other hand, have already taken initial steps with their publications in the area of information security.

Guidelines for more information security in Europe

At the end of November 2019, the EBA published[20] its final "Guidelines for ICT and security risk management".[21] With these guidelines, which are aimed at financial institutions and payment service providers, the EBA has specified "the risk management measures that financial institutions (as defined in paragraph 9 below) must take in accordance with Article 74 of the CRD to manage their ICT and security risks for all activities and that payment service providers (PSPs as defined in paragraph 9 below) must take, in accordance with Article 95(1) of PSD2, to manage the operational and security risks (intended as 'ICT and security risks') relating to the payment services they provide. The guidelines include requirements for

15 See BaFinJournal December 2019 (only available in German), page 11.

16 ESMA, ESA Review, https://www.esma.europa.eu/about-esma/who-we-are/esa-review, retrieved on 20 January 2020.

17 European Commission, Consultation document: A potential initiative on the digital operational resilience in the area of financial services, https://ec.Europe.eu/info/sites/info/files/business_economy_euro/banking_and_finance/documents/2019-financial-services-digital-resilience-consultation-document_en.pdf, retrieved on 7 January 2020.

18 loc. cit. (footnote 3)

19 loc. cit. (footnote 18)

20 EBA, Press release: EBA publishes guidelines on ICT and security risk management, https://eba.europa.eu/regulation-and-policy/internal-governance/guidelines-on-ict-and-security-risk-management, retrieved on 6 May 2020

21 EBA, EBA guidelines on ICT and security risk management, https://eba.europa.eu/sites/default/documents/files/document_library/Publications/guidelines/2020/GLs%20on%20ICT%20and%20security%20risk%20management/872936/Final%20draft%20Guidelines%20on%20ICT%20and%20security%20risk%20management.pdf, retrieved on 8 May 2020.

information security, including cybersecurity, to the extent that the information is held on ICT systems."[22]

As announced in the ESAs' joint advice, EIOPA also launched a consultation at the end of 2019 on a set of draft "Guidelines on Information and Communication Technology (ICT) security and governance".[23] At the moment, it is analysing the responses to the public consultation, which ended in March 2020. The guidelines are directed at insurance undertakings and insurance groups that are subject to the Solvency II regime. As the guidelines were drawn up on the basis of the EBA's draft guidelines, they follow, on the whole, the harmonised regulatory approach proposed in the ESAs' joint advice. As a result, the guidelines are a step forward on the path towards the harmonisation of requirements; a path that BaFin had already embarked on with the BAIT, VAIT and KAIT.

Although both versions of the guidelines cover the same aspects of information security, there are differences in the level of detail and the way in which the requirements are worded. This is due to the specificities of the relevant legislation in place, regulatory approaches and differences between the risk profiles of the entities concerned.[24]

The latter also explains why EIOPA's draft guidelines treat the information security objective of "availability"[25] differently compared to how it is treated in the EBA's final guidelines. In comparison to other entities in the financial sector – such as financial institutions or payment services providers – insurers, and health and life insurers in particular, are less vulnerable to operational disruptions or disruptive attacks. For instance, it is less time-critical that insurers restore the availability of most of their business processes than for payment services providers to ensure the availability of their services.[26]

Generally speaking, the guidelines set out by the EBA and EIOPA place the emphasis on the overall responsibility of the management body as well as on the importance of appropriate budgeting, sufficient resources, and the need to observe the principle of proportionality within the context of the information security requirements. In addition, they both confirm that information security is to be reflected within the system of governance, business strategy, overall risk management system, outsourcing and auditing of the entities concerned.

The EBA sets out in detail how information security risks are to be included in the overall risk management system. While EIOPA in its guideline on ICT and security risks within the risk management system primarily addresses the determination of protection requirements, the section entitled "ICT and security risk management framework" in the EBA's guidelines details the approach to be taken for ICT and security risk management, including the determination of protection requirements, in the risk management framework. This different approach is based on the fact that when setting out its governance requirements, EIOPA focused primarily on information security aspects, which is why the authority does not reiterate general governance requirements in its guidelines. The same is also apparent in the information concerning audits.

Both the EBA's and EIOPA's information security guidelines define high-level principles and rules to protect the confidentiality, integrity and availability of information. On this basis, the entities concerned should establish and implement security measures, such as security monitoring and performing information security reviews, assessments and testing.

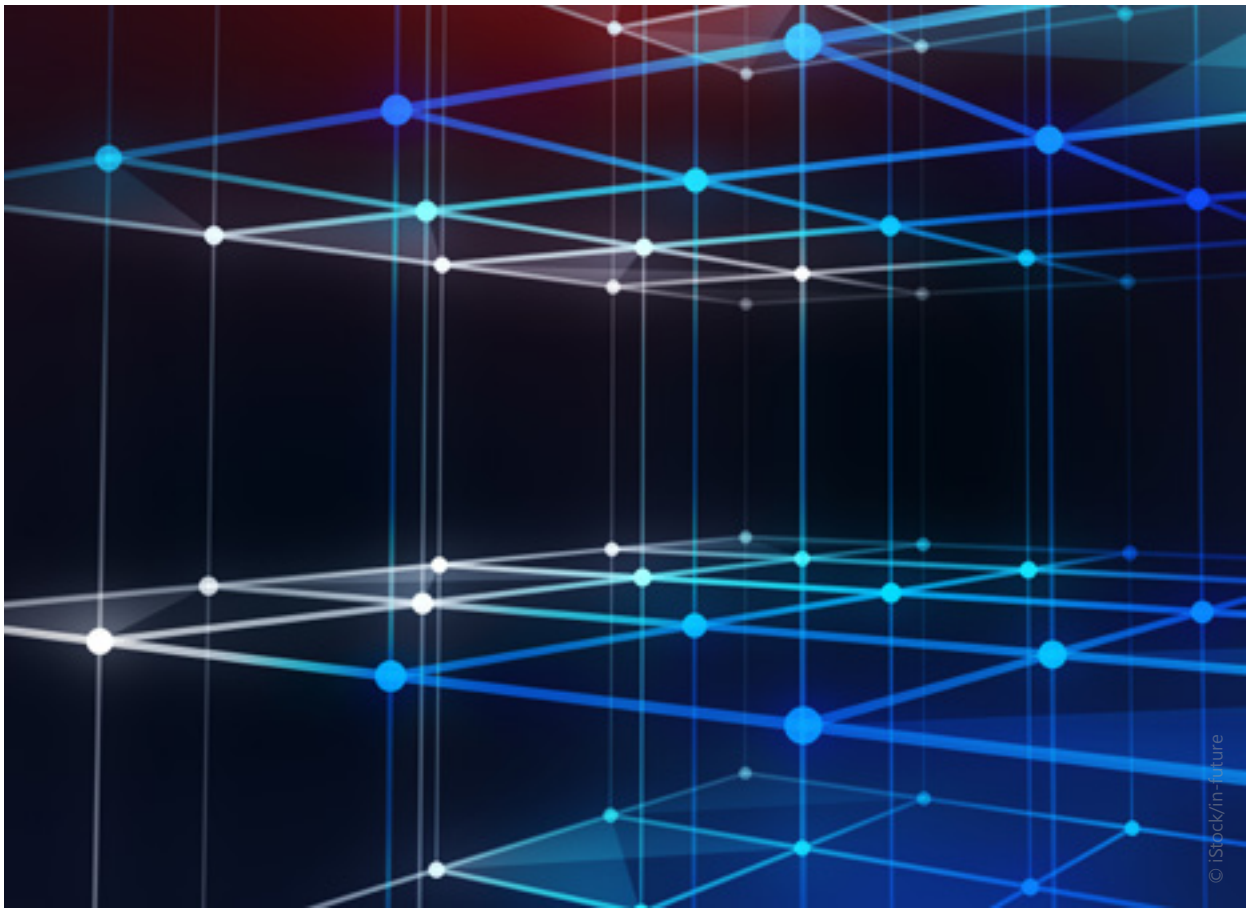
22 loc. cit. (footnote 21), page 6

23 EIOPA, Consultation paper on the proposal for Guidelines on Information and Communication Technology (ICT) security and governance, https://www.eiopa.europa.eu/sites/default/files/publications/consultations/guidelines_ict_security_and_governance_12122019_for_consultation.pdf, retrieved on 6 May 2020.

24 loc. cit. footnote 14, JC 2019 26, page 28 et seq.: Annex B2. ICT security risk profile of an insurance or reinsurance undertaking.

25 Availability: "Property of being accessible and usable on demand (timeliness) by an authorised entity." (source: loc. cit. footnote 24, page 9).

26 loc. cit. (footnote 14, JC 2019 26, page 31, Annex B2, ICT security risk profile of an insurance and reinsurance undertaking.



In the context of the almost identical requirements on security monitoring, entities should identify, continuously monitor and detect anomalous activities that may impact their information security. As part of this continuous monitoring, financial entities should implement appropriate and effective capabilities for detecting and reporting physical or logical intrusion as well as security risks that prevent entities from protecting the confidentiality, integrity and availability of the information assets.

To ensure the effective identification of vulnerabilities in their ICT systems and ICT services, financial entities should perform a variety of information security reviews, assessments and testing. To this end, the entities should establish and implement an information security testing framework and ensure that tests are carried out by independent testers. Details on this information security measure, e.g. regarding testing frequency and the need for a testing framework for payment terminals and devices, are only provided in the EBA's guidelines due to the risk profile of payment services providers and sector-specific regulatory requirements, among other things.

Moreover, the guidelines include further requirements on operations security, project and change management and business continuity management. The latter comprises a business impact analysis (BIA) and business continuity plans (BCP). In the context of business continuity management, entities must develop response and recovery plans, test their BCPs and ensure they have effective crisis communication measures in place. As regards business continuity planning and plan testing, the differences in the EBA's and EIOPA's requirements lie in the details. In the context of business continuity planning, the EBA sets out how to deal with severe business disruptions; in the context of plan testing, the authority's guidelines provide details on the requirements to be met when testing BCPs. EIOPA, on the other hand, does not cover these two aspects due to the specific risk profile of insurance undertakings, particularly in relation to the information security objective of availability, and its specific regulatory approach when drafting guidelines.

Overall, it can be concluded that both the EBA and EIOPA guidelines follow a clear harmonisation approach that is expected to continue at the level of European Directives. In the meantime, until this European project is completed, both of these sets of guidelines will make a significant contribution towards setting out what both EBA and EIOPA expect the entities they supervise to achieve in the area of information security.

4 Harmonisation of regulatory requirements for outsourcing to cloud service providers

Framework for the oversight of critical service providers

The European Supervisory Authorities (ESAs) have published a joint opinion on outsourcing to cloud service providers. In this opinion, they highlighted the need for a common legal framework for the oversight of critical service providers.

This framework is to provide an overview of the risks associated with outsourcing to third parties that supervised entities and the financial market as a whole face.

A legal framework should thus define the criteria for considering when a third party provider is "critical". It should be noted that third party providers operate across borders both within and outside the European Union. For this reason, the ESAs consider international coordination to be desirable.[27]

In this context, the ESAs focus particularly on cloud service providers (CSPs) as the subject of such oversight for monitoring critical service providers. According to the ESAs, only a small number of CSPs currently serve most of the financial market. As a result, if one of these service providers were subject to a serious breach, it could have an impact on the stability of the financial sector as a whole.

The harmonisation and consistency of supervisory requirements for information security is also a matter of great importance in the context of outsourcing to CSPs in the financial sector. However, there is a certain amount of uncertainty among supervised entities in relation to the implementation of requirements under supervisory law. For this reason, the European Commission included in the FinTech action plan its call on the ESAs to determine whether there is a need for guidelines on outsourcing to CSPs.

27 JC 2019 26, pages 4 and 18.

The ESAs' approaches: recommendations and guidelines

At the European level, EIOPA, the EBA, the Single Supervisory Mechanism (SSM) and NCAs have been regularly sharing information in recent years on how to deal with outsourcing to cloud service providers. In 2018, the EBA addressed the growing need for guidance and was the first European Supervisory Authority to publish "Recommendations on outsourcing to cloud service providers".[28] In doing so, it took an important step towards more transparency on the use of cloud services. EIOPA and ESMA are following this European line of approach.

Last year, the EBA included these cloud-specific recommendations in its general "Guidelines on outsourcing arrangements"[29] (see info box, page 31). For this reason, the "Recommendations on outsourcing to cloud service providers" ceased to apply with effect from 30 September 2019. The other ESAs are continuing to work on their cloud-specific recommendations for action.

EIOPA and ESMA have thus taken a leaf out of the EBA's book. Following a consultation phase last year, EIOPA published its "Guidelines on outsourcing to cloud service providers" in February.[30] ESMA, too, started working on such guidelines last year. In this context, EIOPA and ESMA stated that they seek to make their guidelines

28 EBA, Recommendations on outsourcing to cloud service providers, https://eba.europa.eu/sites/default/documents/files/documents/10180/2170121/5fa5cdde-3219-4e95-946d-0c0d05494362/Final%20draft%20Recommendations%20on%20Cloud%20Outsourcing%20(EBA-Rec-2017-03).pdf, retrieved on 10 March 2020.

29 EBA, Guidelines on outsourcing arrangements, https://eba.europa.eu/sites/default/documents/files/documents/10180/2551996/38c80601-f5d7-4855-8ba3-702423665479/EBA%20revised%20Guidelines%20on%20outsourcing%20arrangements.pdf, retrieved on 10 March 2020.

30 EIOPA, Guidelines on outsourcing to cloud service providers, https://www.eiopa.europa.eu/content/guidelines-outsourcing-cloud-service-providers_en, retrieved on 29 April 2020.

consistent with the EBA's proposals unless there is a need to deviate from the provisions due to the specific features of each individual area of supervision.

The ESAs are thus following a harmonised and coherent regulatory approach for the publication of guidelines for outsourcing to cloud service providers – even if these guidelines are published in separate documents. The objective is to offer financial entities clarity on the ESAs' expectations and thus make it easier for these entities to implement the requirements.

At a glance

EBA guidelines on outsourcing arrangements

The EBA guidelines entered into force on 30 September 2019 and replaced both the outsourcing guidelines that had been applicable up to that point, which had been set out in 2006 by the EBA's predecessor (CEBS),[31] and the EBA's 2017 "Recommendations on outsourcing to cloud service providers". In these new guidelines, the EBA specified its expectations with regard to outsourcing arrangements. Here, the EU authority emphasised in particular that each financial institution's management body remains responsible for that institution and all of its activities, at all times. The EBA identified outsourcing to service providers located in third countries as a major risk. In such cases, institutions must ensure that EU legislation and regulatory requirements, e.g. in the area of data protection, are complied with. Consequently, this also affects sub-outsourcing.

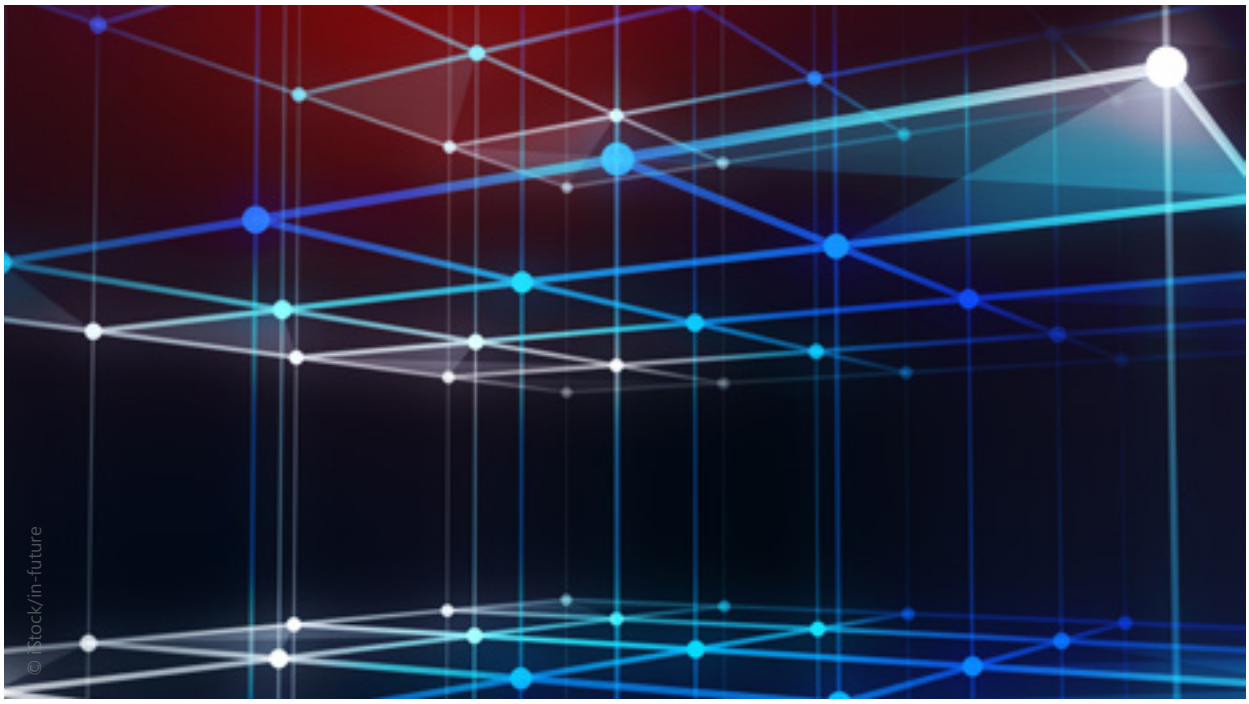
The guidelines also bring a number of changes: for example, institutions are required to maintain a register of all existing outsourcing arrangements. Moreover, institutions must inform NCAs of any new plans to outsource critical or important functions in addition to material changes and/or severe events. The guidelines also set out access, information and audit rights for NCAs and institutions in all outsourcing arrangements. As regards the outsourcing of functions that are not critical or important, institutions are only required to ensure these rights using a risk-based approach. Financial institutions must set out these access, information and audit rights in writing in their agreements with service providers. Existing contracts must be amended to reflect the new guidelines.

BaFin's approach: Guidance on outsourcing to cloud service providers

While the EBA, EIOPA and ESMA have published their own recommendations/guidelines on outsourcing to cloud service providers step by step or are planning on releasing such documents, BaFin published its "Guidance on outsourcing to cloud service providers" ("*Merkblatt – Orientierungshilfe zu Auslagerungen an Cloud-Anbieter*") in November 2018, covering all the areas under its supervision. This guidance notice is in line with European efforts towards the harmonisation and consistency of supervisory requirements,[32] as it contains recommendations that are aimed at supervised entities in the financial sector (credit institutions, financial services institutions, insurance undertakings, pension funds, investment services enterprises, asset

31 The Committee of European Banking Supervisors was part of the European Union's Lamfalussy process.

32 See BaFinJournal April 2018 (only available in German), page 29 et seq. and https://www.bafin.de/dok/13003422



management companies, payment institutions and e-money institutions) and are thus to be interpreted within the context of the applicable requirements under supervisory law. The recommendations focus on the supervisory practices currently adopted by BaFin and the Deutsche Bundesbank in such cloud-specific cases of outsourcing and they are aimed at providing assistance and raising awareness of issues that may arise when using cloud services and implementing the relevant requirements under supervisory law.

In addition to providing information on cloud-specific aspects in the context of risk analysis, the focus also lies on contractual arrangements in particular. In the course of its ongoing supervisory activities, BaFin found that financial entities experienced significant difficulties when drafting contracts with service providers. Cloud service providers offering services primarily to other sectors also initially faced some challenges due to the supervisory requirements that apply in a highly regulated financial market. BaFin's "Guidance on outsourcing to cloud service providers" has provided some clarity here. In addition, BaFin's Guidance offers transparency, also for cloud service providers, in relation to contractual terms granting supervisors unrestricted information and audit rights. This, too, has had a positive impact on contract negotiations for supervised entities.

BaFin's Guidance also provides information on how audit activities can be structured in a more efficient and simple way. For example, pooled audits may be conducted. In this context, the internal audit function of one or multiple outsourcing financial entities supervised by BaFin may jointly exercise their information and audit rights vis-à-vis cloud service providers. This has been well-received in the financial industry: *Deutsche Börse*, for instance, launched the Collaborative Cloud Audit Group (CCAG) in 2017. This industry-wide initiative involving several large European financial institutions and insurers has already conducted audits at global cloud service providers such as Microsoft on behalf of the initiative's members.[33] This demonstrates that the contractually agreed information and audit rights of financial entities can be exercised in practice.

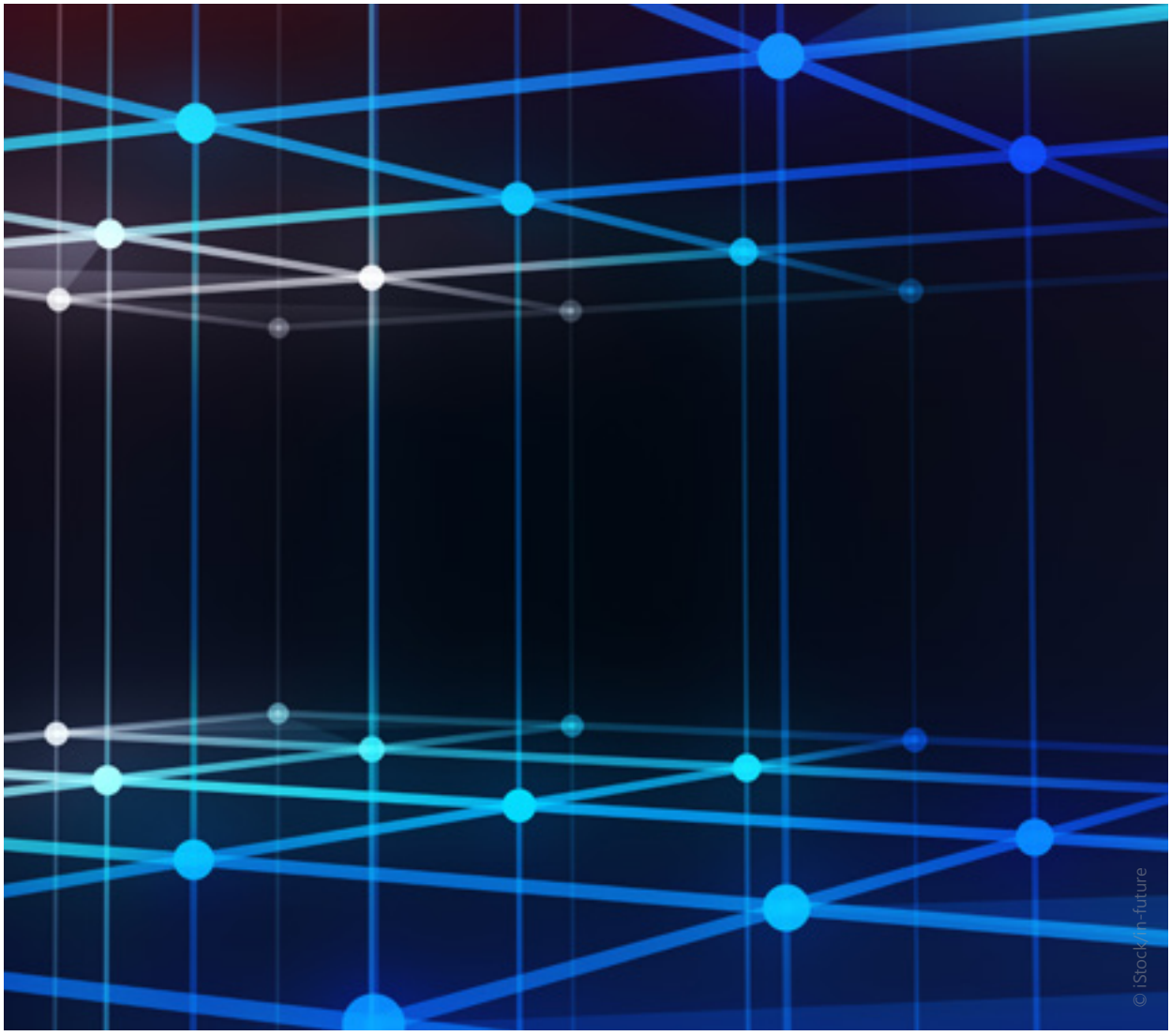
BaFin is planning on taking further supervisory measures in the area of cloud computing. The reason for this is that the pooled audits that have been conducted at cloud service providers have shown that audits in third countries in particular are a challenge for supervised entities. This is because these require considerable staff and financial resources. BaFin is therefore in favour of new regulatory standards at the European level in order to make the situation easier both for supervised entities and financial supervisors.

33 Deutsche Börse Group press release: Deutsche Börse and Microsoft reach a significant milestone for cloud adoption in the financial services industry, https://www.deutsche-boerse.com/dbg-en/media/press-releases/Deutsche-B-rse-and-Microsoft-reach-a-significant-milestone-for-cloud-adoption-in-the-financial-services-industry-1540058, retrieved on 29 January 2020.

5 Conclusion

The European Commission, the European Supervisory Authorities and BaFin, as Germany's financial supervisory authority, all attach great importance to the harmonisation and convergence of supervisory requirements for information security and cloud computing at the national and European level.

With its BAIT, VAIT and KAIT circulars, BaFin published harmonised information security requirements for large parts of the financial industry at an early stage while taking into account the aspects that are specific to each sector. In doing so, BaFin plays a leading role here in the European context. With its "Guidance on outsourcing to cloud service providers", BaFin went one step further by setting universal requirements that apply to all the entities under its supervision. And with its publications, BaFin is addressing the ever-growing importance of digital operational resilience and the associated need for harmonisation and regulation – also within the European context.



II

Cyber resilience and crisis management – a task for institutions and supervisors

How German banks are gearing up for the fight against cybercrime

Authors

Andreas Krautscheid
Chief Executive of the Association of German Banks (*Bundesverband deutscher Banken*)

André Nash
Associate Director, Banking Technology and Security Group, Association of German Banks (*Bundesverband deutscher Banken*)

1 Introduction

The coronavirus crisis has once again shown us that banks play a key role and carry great responsibility in the economy. Banking operations need to run properly, and disturbances and disruptions on a massive scale must be prevented at all costs.

In recent years, the risk of cyberattacks on the German economy and thus on the financial sector has increased dramatically. There are two obvious reasons for this: firstly, the digital transformation of all areas of social and economic activity and the growing interconnectedness of companies, which is opening up new gateways for hackers; secondly, cybercriminals are becoming increasingly professional and are continuously beefing up their arsenal of tech weapons. There is a reason why cyberattacks are currently considered the most significant operational risk in the financial sector.

The digital systems of many companies, not least credit institutions, are so complex nowadays that it is simply impossible to completely prevent attacks from happening. In addition, the progress that is being made in the area of artificial intelligence (AI) is allowing for new and perfected attacks. To give an example, there was a rise in telephone fraud cases last year where criminals would use AI to mimic voices in order to scam company staff and obtain money. A significant increase in the use of deepfakes, including fake videos, is anticipated for 2020. In this case, AI is used as a means to radically modify data. However, these systems will not be carrying out such attacks autonomously for the time being, as human intelligence is still required to a significant extent in order to find security vulnerabilities, prepare attack scenarios and carry out attacks.

While humans will remain the ones actively taking advantage of security vulnerabilities for now, autonomous AI-based systems are particularly good at spotting software bugs[1] and tackling them. We can see where this trend may be heading based on the following real-life example: During a DARPA[2] hacker conference, a system was presented in a pre-prepared test environment; this system found a software bug that the event host was unaware of and it launched a successful attack on another system. A third system observed what was happening, reverse engineered the attack, found the bug, wrote a patch[3] and installed it onto its own system – all within 20 minutes. This is not yet the case everywhere but we can already see how these approaches will evolve.

There is another potential source of risk: banks have been increasingly outsourcing their IT systems to a relatively small number of IT services providers. They are also increasingly making use of cloud services. If these service providers experience a disruption or restricted availability due to a cyberattack, this could have serious consequences. To continue with the example of the cloud, the advantages and potential associated with incorporating cloud solutions into banking processes and systems are obvious. But as there is just about a handful of key global cloud service providers, there is a risk that a large number of banking systems are running on just a few cloud systems. And even though individual cloud systems are able to spread the risk of disruptions via a network architecture to such an extent that such disruptions are almost impossible, there can still be outages in practice. For instance, several Google Cloud services experienced a temporary outage in the summer of 2019. To sum up the above, there is not only a financial or reputational risk for individual banks but also a systemic risk for the financial sector as a whole. For this reason, we need the entire financial system to analyse the threat situation on an ongoing basis and take measures in a coordinated manner.

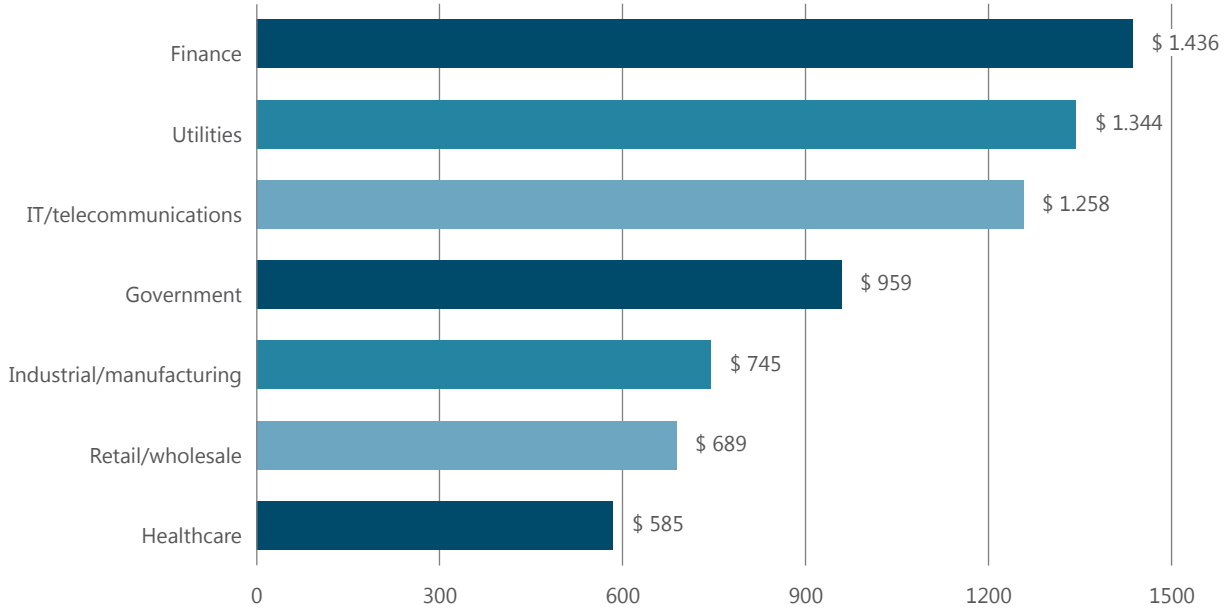
1 A software bug is an error, flaw or fault that can result in computer programme errors or security vulnerabilities.
2 DARPA stands for Defense Advanced Research Projects Agency. DARPA is an authority that is part of the United States Department of Defense. It conducts research projects for the United States Armed Forces.
3 A patch is a set of changes to software aimed at fixing any errors or security vulnerabilities that have been identified or adding functions that were not yet available.

2 Decades of expertise - banks have been involved since day one

Cyber risk poses a challenge for the banking industry as a whole – and this challenge is to be taken seriously. However, credit institutions also have the particular expertise they need to protect their technical infrastructures. Cyber attacks have been a key issue for our member banks since the launch of online banking in November 1980, almost 40 years ago. The ongoing improvement of security systems to protect customer data and ensure customer trust has been one of the top priorities for banks for a long time now. This is also reflected in the investments that are made in this area. According to a global survey conducted by the cybersecurity company Kaspersky Lab, banks are in first place in terms of investments in IT security per head.[4]

4 Kaspersky Lab Security Economics Report, page 12.

Figure 1: Expenditure on IT security per head



Source: Kaspersky Lab Corporate IT Security Risks Survey

3 Human behaviour as a risk factor

However, the most secure technological system may not offer sufficient protection if those using the system do not respect basic security requirements. In fact, human behaviour might be the biggest gateway for cyber attacks. Weak points include individuals and their login data, which cybercriminals use to try to access accounts or banking systems. Attacks range from phishing[5] e-mails sent to a large number of people to targeted attacks on specific individuals who may have been spied on for months (spear phishing attacks). This is why banks are making a significant effort to launch campaigns to raise awareness and to provide training and information to staff and customers on an ongoing basis.

5 Phishing is defined as the fraudulent attempt to obtain the personal data of an internet user for the purpose of identity theft via fake websites, e-mails or instant messaging.

4 Growing importance of information-sharing and networks

Connecting cybersecurity managers across companies and sectors has become just as important as their IT expertise. Sharing information is a key tool to ensure protection against and tackle cyberattacks. Informing the community quickly of an attack that is taking place allows the industry to be on high alert and to rapidly adapt defence mechanisms based on the attack vectors in question. Exchanging information on incidents that have been analysed is crucial for banks in order to ensure the best possible protection. Malware can sometimes remain hidden for weeks or even months. Damage can then be inflicted if the malicious software is activated and the attack is carried out – triggering the defence mechanisms in place. But if this software can be identified in advance with system analyses – based on information that has been shared – this can help to tackle and predict further potential attacks. Moreover, this information makes a significant contribution towards preventing further attacks as it becomes part of ongoing training for staff and IT security experts. The data that is gathered on these attacks is also relevant for prosecutors, as it is not rare for such data to facilitate the arrest of cybercriminals.

However, it should be noted that the exchange of information on a voluntary and regular basis between banks, security authorities and prosecuting authorities is not enough. A vast amount of unfiltered information on current attacks, new malware and ongoing phishing campaigns is often released on various platforms. As there is a huge number of cyber activities worldwide, the quantity of raw data is so large that one may

wonder how useful this data is. This is because before information can be incorporated into a bank's defence mechanisms, attacks need to be analysed and defence measures need to be evaluated and adapted to the bank's systems in order to prevent new risks. For this reason, there is a need for better filtered and pre-analysed information that is relevant to the company's own systems, and this information needs to be available as quickly as possible.

There is another problem: regrettably, the growing complexity of IT security regulation in the financial sector is causing uncertainty on what information may (still) be shared with whom. In order to improve the ways in which information is shared, also on a cross-border basis, it would be worth addressing inconsistencies and provisions that are open to interpretation, especially if this concerns personal data. The financial services sector is therefore seeking legal certainty on how financial institutions can exchange information on threats within the industry. We need common EU-wide framework conditions that clearly allow certain information and findings to be shared between private organisations and the private and public sectors. As a general rule, it is essential that public sector and private sector security incident and reaction teams at companies and (security) authorities are able to closely interact in order to ensure that potentially serious incidents can be dealt with. Security incident detection and analysis and crisis response (where applicable) are a common task and must be dealt with as such.

5 Regulatory measures must be harmonised

The growing number of cyber attacks on banks in recent years has also become an increasingly significant issue for supervisory authorities as this could jeopardise the stability of the financial sector. At the European level, the European Central Bank (ECB) and the European Banking Authority (EBA) have specified their expectations on how to increase cyber resilience in the financial sector. And at EU level, the European Council and the European Parliament have adopted the Directive on security of network and information systems (the NIS Directive), the Second Payment Services Directive (PSD2) and the Cybersecurity Act.

The supervisory requirements in place are largely consistent with the banks' efforts and activities in this regard. However, the regulatory requirements set by the individual supervisory authorities are often not harmonised. This leads to a considerable workload for credit institutions. Banks are required to provide evidence to each individual authority to demonstrate that the requirements are met. In addition, they must answer an extensive list of questions and report the same information in different forms to different authorities. It is clear that this is not the best solution. It would be far more efficient to allocate the resources that are needed for this to the defence mechanisms directly. For this reason, it is absolutely necessary that the requirements are harmonised and that an organised reporting system for providing evidence and reporting is set up. This would result in a higher security level overall, appropriate supervisory practices and less bureaucracy. The European Commission's current public consultation to improve cyber resilience[6] shows that financial supervisors and politicians are well aware of this issue. But what will be the outcome? It would not be good news if this resulted in new requirements for banks but did not bring about the much-needed reduction in complexity.

Moreover, harmonisation is a key issue in the context of Threat Intelligence-based Ethical Red Teaming, i.e. TIBER testing, as well. These simulated hacker attacks are based on a framework set by the European Central Bank – and while the ECB is focusing on financial market infrastructures, national central banks and supervisory authorities are implementing this test approach for the banks in the individual EU Member States. However, we can currently see that there are many aspects that remain unclear – e.g. in relation to the possible certification of testing companies (Red Teams) or the comparability of the individual national tests. To achieve the desired level of harmonisation, it would be important to ensure that a test that has been conducted in one country is recognised by other EU Member States to avoid conducting the same test twice and to avoid unnecessary extra work. It is also crucial for global banks to ensure that the TIBER tests can be compared – and ideally recognised – despite different testing approaches in countries outside the EU, such as the approach used in the Bank of England's CBEST framework.

6 European Commission, Digital Operational Resilience Framework for financial services: Making the EU financial sector more secure, https://ec.europa.eu/info/sites/info/files/business_economy_euro/banking_and_finance/documents/2019-financial-services-digital-resilience-consultation-document_en.pdf, retrieved on 27 April 2020.

6 National and international cooperation is needed to win technological race

It is becoming clear that banks need to be prepared to face far more sophisticated and potentially large-scale cyber attacks in 2020 than in the past. As hackers are making technological progress and have now reached the level of national security authorities, we all need to join forces. It is only when knowledge is shared and innovation is promoted that we can succeed in being ahead of those seeking to do harm. The global aspect of this must not be overlooked. Cyber attacks on banks can be launched anywhere around the world – and this can have a global impact on the financial system. For this reason, the only way forward is coordinated action at the international level. Banks, the security industry and the national and supranational authorities concerned must all pull together.

Solutions to problems that do not exist yet

Author

Professor Dr. Igor Podebrad
Head of Cyber Risk and Information Security and Group Chief Information Security Officer, Commerzbank AG

1 Cyber resilience as a key element of IT security strategy

The Emotet[1] Trojan continues to wreak havoc in large areas of the economy. Once infecting a company's IT system, this destructive malware, which poses a global threat, allows other malware to be downloaded, leading to data outflows and enabling criminal hackers to gain full control over the complete IT system.

As a result of such attacks, the IT systems of a large number of companies and public institutions, such as hospitals, were severely disrupted and in some cases brought to a complete standstill. This led to production downtime in the industry lasting several days. The Court of Appeal (*Kammergericht*) in Berlin, for example, encountered a malicious software event of this kind in September 2019 and had not been able to fully restore its digital infrastructure for months.[2]

European banks for their part have managed to prevent significant damage caused by cyber security incidents – for the time being at least – with only a small number of institutions being seriously affected by an Emotet attack. Nevertheless, this malware makes it patently clear to us at banks and other financial institutions that relying on prevention alone is not enough.

As cyber attacks are becoming increasingly sophisticated, major security incidents can never be ruled out entirely. While the risk of occurrence can and must be greatly reduced by means of technical measures and increased staff awareness, far more needs to be done to shield from attack.

For the day will surely come when a malware-infected email sneaks its way past the spam and virus scanners and unleashes its destructive content by a staff member inadvertently clicking on the link, no matter how much security awareness training that person has received. To keep potential damage to a minimum if such a cyber attack occurs, a forward-looking security architecture must be installed in order to detect and identify the infection and reduce the risk of contagion as quickly as possible so that the process of data restoration can begin.

It is therefore essential that financial institutions organise their operations in such a way that continuity is assured in case of disruption and that any loss of operability is kept to a minimum.

1 More information on Emotet can be found on pages 13 et seq. and 17.
2 Berliner Morgenpost, Cyberangriff auf Berliner Kammergericht: Ein Protokoll (Cyber attack on the Berlin Court of Appeal: a report), https://www.morgenpost.de/berlin/article228301127/Cyberangriff-auf-Berliner-Kammergericht-Ein-Protokoll.html, retrieved on 17 April 2020. Editor's note: The Court of Appeal had still not been able to go fully digital by the time the original German version of this article went to press.

2 Cyber risks must be managed in the same way as all other material risk types

Cyber resilience, in other words an entity's ability to withstand attacks, is a key element of a bank's IT security strategy. The responsibility for this lies with the Chief Information Security Officer (CISO). Their task in times of cyber risks, fake news and the coronavirus pandemic is to strike a balance between maintaining operational stability and satisfying additional requirements for IT security.

This requires radical rethinking on the part of management which must always take the possibility of a major cyber event or disruption into account from the outset. It is therefore not sufficient to consider only individual areas of the technical systems.

The focus must be on institutions knowing how they should deal with unforeseen disruptions before they even occur. Business processes, entire business units, organisational matters and corporate governance and culture must be considered and correspondingly aligned within this context.

Moreover, BaFin's banking supervisors attach great importance to this focus, which is now reflected in its supervisory practice. Supervisors and regulators expect financial institutions to manage cyber risks in the same way as they do all other material risk types.

The reason for this is that cyber risks affect all areas and have a major influence on the entire risk situation of a bank. Cyber risks should therefore be rigorously and consistently monitored and modelled according to their operational, technical, financial and reputational risk potential along with all other types of risk that the bank faces.

Both organisationally and in terms of responsibilities, the CISO therefore ideally reports to the Chief Risk Officer. For if decisions have to be made in response to a cyber attack, the CISO must be very quick to act and often has to adopt a different course of action to that originally planned. After all, the threat environment is extremely dynamic and the precise measures needed to counter them are difficult to plan in advance.

Agility is therefore crucial to an organisation's cyber resilience. To achieve this, the CISO needs sufficient information to ensure that cyber occurrences are appropriately monitored and managed. Cyber resilience also means that software tests and operational procedures are automated and integrated as far as possible.

3 Clients' cyber resilience is taken into account in the risk evaluation

Cyber risks are difficult to forecast and therefore difficult to model. Unlike established risk data, the availability of historical, statistically valid data is low. In addition, the likelihood of such events occurring is minimal compared with the extreme damage they can cause.

Compounding this is the enormous pressure facing banks to modernise and remain competitive. Institutions must respond very quickly to market changes and launch products that have not yet reached full maturity. "Time to market"[3] is the new watchword in the digital age. Faced with the pressure to deliver, there is a greater willingness to accept a higher degree of error risk. This naturally poses a challenge from an IT security point of view. For errors can open the door to cyber attacks which must then be mitigated with other countermeasures and processes.

A bank's cyber security strategy also includes all of its clients' processes. It is important to ensure that the security and resilience of the supply chains of business partners can be verified in a transparent way.

Our clients can benefit from this expertise. We at Commerzbank sharpen their awareness for these topics and, by so doing, contribute to both their security and ours. Our clients' cyber resilience is also a factor that is taken into account in the bank's risk evaluation.

Business email compromise attacks can be used as an example to illustrate the importance of heightened awareness in the area of IT security, specifically the CEO spam. By sending out emails or making telephone calls, cyber criminals trick employees into thinking that they are dealing with the CEO, prompting them to make a payment, only to find out that this was a scam. An employee who feels part of a trusting and appreciative corporate culture is more likely to personally contact the person supposedly commissioning the payment, if there is any doubt surrounding the authenticity of the payment order.

3 Time to market is the length of time it takes from a product being conceived until its being available for sale.

4 Cyber regulation should not be allowed to get out of hand

Online activity in business and society has now reached such a level that government regulation has become imperative.

Regulation is both important and the right approach. However, as the number of cyber security provisions is steadily rising, companies are increasingly overwhelmed by the flood of provisions with which they must comply and which are often similar but in some cases inconsistent. Examples are contradictions between data protection laws and IT security laws, and inconsistencies between sectoral and cross-sectoral rules. In addition, there are national regulations that are incompatible with those of other countries, duplicative regulations and multiple reporting processes to different authorities for one and the same event simply because the forms to be used differ slightly.

As cyber criminals do not confine their attacks to national borders, a level playing field based on internationally applicable rules is needed.

The European Central Bank's cyber security framework, TIBER-EU,[4] seeks to achieve greater cyber resilience for financial institutions across Europe. The ECB uses this framework to launch controlled cyber attacks against an institution's IT system in order to test the ability of that system to withstand such attacks.

The red teams that simulate the attacks not only sound out the weak spots of an institution's IT infrastructure; they also test human factors by carrying out social engineering attacks. These tests are very extensive and take many months to complete. Non-European jurisdictions are also turning to red teaming as a means of testing their critical infrastructures. It is important that these tests are mutually recognised as being standard procedure.

However, cyber regulation should not be allowed to get out of hand. It is clear where the main regulatory focus should lie – on transparent risk management, cutting-edge security measures, incident reporting, cooperation between the state and industry. Legislators, enterprises, scientists and academics must set out a transatlantic framework that can serve as a foundation for cyber security in Europe and the USA – and act as role model for the rest of the world.

4 For more information, see page 47 et seq.

5 Cyber security under threat from new technologies

New technologies, such as biometry, artificial intelligence and quantum computers, are close to or have already achieved a breakthrough. However, the new technological possibilities also give rise to new forms of cyber security threats.

Quantum computing[5], for example, has the potential to render many widely used security procedures useless.

This is why we make decisions today to ensure that tomorrow's threats are adequately addressed.

This forward-looking approach does not always meet with acceptance and support within a company. Why should we be working towards solutions to problems that do not exist yet? Because, as is so often the case, the future is there long before most of us realise it.

5 Quantum computing refers to performing tasks using quantum computers. These computers employ quantum-mechanical effects in order to store and process data.

Cyber resilience with TIBER-DE – A future framework for ethical hacker attacks on financial entities in Germany

Authors

Silke Brüggemann
Senior Advisor, Division for Policy Issues relating to IT Supervision and Inspections, BaFin

Dr. Miriam Sinn
Head of the TIBER Cyber Team Germany, *Deutsche Bundesbank*

Christoph Ruckert
Senior Advisor, Division for Policy Issues relating to IT Supervision and Inspections, BaFin

1 Introduction

As a result of increasing digitalisation in the financial sector and the threat of cyber attacks on banks, insurers and financial market infrastructures, the focus is shifting more and more to the ability of these entities and their most important service providers to withstand internal and external attacks.

For this reason, the European Central Bank (ECB) published the sector-independent and entity-independent TIBER-EU Framework (TIBER: Threat Intelligence-based Ethical Red Teaming) in May 2018. The objectives of the framework are to promote an adequate level of cyber resilience (see info box on page 48) for the entities as a key factor that will ensure the proper functioning, stability and integrity of the financial system, and to enable the results of such penetration tests to be compared and mutually recognised in the European context.

TIBER tests are an effective way of further increasing the cyber resilience of entities that already have a high

level of information security. This sort of test involves commissioning external "ethical hackers" to carry out simulated attacks on an entity. The objective is to test how effectively the entity can prevent, detect and respond to cyber attacks, using information obtained beforehand about the security threats faced by the entity and applying tools used by professional hackers. The test focuses explicitly on the entity's critical functions. Unlike conventional penetration testing, TIBER tests are not aimed solely at technical vulnerabilities – they also incorporate the human factor into the attack scenarios.

Definition

Cyber resilience

The term "cyber resilience" describes an entity's ability to withstand attacks on the security of its information and communications technology (ICT). Hackers focus on an entity's systems or even customer data.[1]

1 See expert articles from BaFinJournal on the BaFin website dated 13 May, Focus on cyber resilience, https://www.bafin.de/dok/12451900, and 23 October, 14 September - Not just another day, https://www.bafin.de/dok/13129070.

2 Implementation in other countries

The TIBER-EU Framework has been implemented in Belgium, Denmark, Ireland and the Netherlands so far.[2] As the first national implementation, the Dutch framework TIBER-NL[3] has served to inspire other national programmes in many ways.[4] Other countries have announced an implementation or are taking specific steps towards implementation.

Initial experience with TIBER tests in the Netherlands has shown TIBER to be a promising concept for implementing threat-led penetration testing. The target group was first limited to financial institutions and their critical infrastructure; it has since been expanded to include insurance companies and pension funds. The Netherlands has even already had an initial pilot project in the energy sector.[5]

Another positive development in the Netherlands has been that of TIBER networks, linking together the entities that have participated in a TIBER test. These networks are helping to build the trust and cooperation necessary for TIBER testing to be performed in the industry. In Germany, the aim is also to learn from other countries' experiences when implementing the test.

The Deutsche Bundesbank and BaFin are developing TIBER-DE based on the TIBER-EU Framework and other countries' experiences in implementing the tests on a national level, taking into consideration the European Supervisory Authorities' "Joint Advice on the costs and benefits of a coherent cyber resilience testing framework for significant market participants and infrastructures within the EU financial sector".[6,7] Publication is planned for 2020.

2 As at 27 November 2019.

3 TIBER-NL GUIDE – How to conduct the TIBER-NL test, November 2017, https://www.dnb.nl/binaries/TIBER-NL Guide Second Test Round final_tcm46-365455.pdf, retrieved on 3 December 2019.

4 TIBER-NL goes Europe, https://www.dnb.nl/en/news/nieuwsbrief-betalingsverkeer/Juni2018/index.jsp, retrieved on 3 December 2019.

5 DNBulletin: DNB's TIBER programme: the next steps, https://www.dnb.nl/en/news/news-and-archive/DNBulletin2018/dnb379565.jsp, retrieved on 3 December 2019.

6 Joint Advice on the costs and benefits of a coherent cyber resilience testing framework for significant market participants and infrastructures within the EU financial sector, https://eiopa.europa.eu/Publications/JC%202019%2025%20(Joint%20ESAs%20Advice%20on%20a%20coherent%20cyber%20resilience%20testing%20framework).pdf, retrieved on 3 December 2019.

7 See expert article from BaFinJournal on the BaFin website dated 13 May, Focus on cyber resilience, https://www.bafin.de/dok/12451900.

3 National framework: TIBER-DE

Credit institutions, insurers, financial market infrastructures and their critical service providers are to be given the opportunity to conduct TIBER-DE tests on a voluntary basis. However, the most important entities in the financial sector are expected to utilise this innovative instrument and thus contribute to the cyber resilience of the entire sector.

As part of the implementation of the European framework in Germany (see figure 1, page 51), the expert team tasked with conducting TIBER-DE tests on the national level, called the TIBER Cyber Team (TCT – see info box), will be based at the Deutsche Bundesbank as part of the Payment and Settlement Systems Directorate General – an area that is not engaged in supervisory activities and is thus outside the realm of banking supervision.[8] Since TIBER-DE has generally been designed to be a voluntary instrument, the Bundesbank has made a clear organisational distinction between TIBER-DE and its banking supervision in-house. This will ensure that the supervisors obtain information only through the designated channels.

TIBER-DE will be managed by a steering committee with members from BaFin and the Deutsche Bundesbank. The committee, currently working intensively on the exact structure of the TIBER-DE framework, is also in charge of defining strategic objectives and further developing TIBER-DE. Due to its strategic focus, the steering committee will not be involved in the individual TIBER-DE tests.

The basis for the national implementation of TIBER-EU is the TIBER-EU Framework[9], which describes the procedure of adapting and implementing the framework on the national level as well as the individual phases, activities and documents to be prepared for a TIBER test.

Definition

TIBER Cyber Team

The TIBER Cyber Team (TCT) acts as a centralised team of experts for a TIBER implementation at national level. In Germany, the TCT is based at the Bundesbank. Throughout the course of the TIBER tests commissioned by entities, the TCT provides support and specialist knowledge, ensures that the TIBER test framework conditions are met and acts as the contact point for all external enquiries. The TCT is entitled to classify a test as non-TIBER-conform if it has not been conducted in line with its requirements.

The Team Test Manager (TTM) is the TCT member in charge of a specific entity in the context of a TIBER test, serving as the interface to that entity. The TTM advises the entity throughout the duration of a test.

The TIBER test process consists of one optional phase and three mandatory phases (see figure 1), shown on page 51.

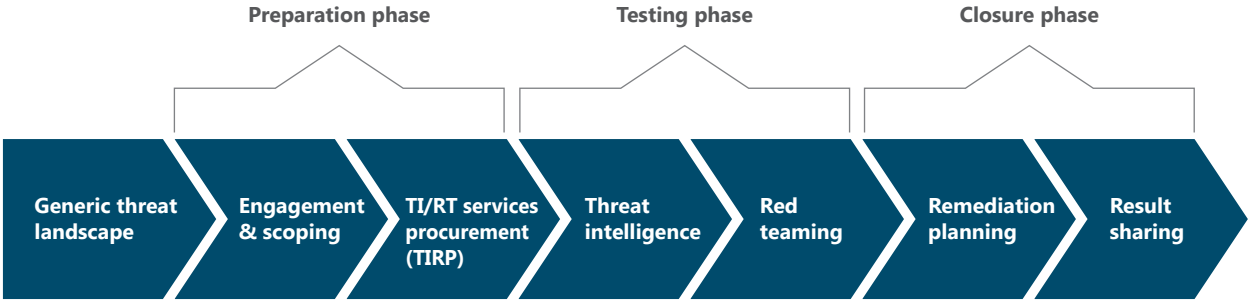
Generic threat landscape
The (optional) generic threat landscape phase involves assessing the situation in terms of risks and threats for the entire (national) financial sector. Relevant potential threat actors and their specific techniques, tactics and approaches are analysed in terms of their underlying principles. The specific approach to be taken for developing the generic threat landscape will be discussed in the further course of the implementation of TIBER-DE.

Preparation phase
During the preparation phase, planning begins for the TIBER test; the launch meeting involving the TIBER Cyber Team – and, optionally, BaFin – is held, the scope of the test is established and the entity commissions the external test service providers.

8 Press release "TIBER-DE enhances the security of the German financial system", https://www.bundesfinanzministerium.de/Content/EN/Pressemitteilungen/2019/2019-11-09-joint-release-with-bundesbank.html, retrieved on 3 December 2019.

9 TIBER-EU FRAMEWORK – How to implement the European framework for Threat Intelligence-based Ethical Red Teaming, May 2018, https://www.ecb.europa.eu/pub/pdf/other/ecb.tiber_eu_framework.en.pdf, retrieved on 3 December 2019.

Figure 1: The TIBER-EU process



Source: European Central Bank, TIBER-EU Framework, May 2018, page 20, figure 3.

The Deutsche Bundesbank appoints the TIBER Test Manager (TTM) from the TIBER Cyber Team to be the point of contact responsible for the entity, which in turn sets up the White Team (WT)[10].

The White Team is the team within the entity being tested that is responsible for the overall planning and management of a TIBER-DE test; the WT is appointed by the entity's board and serves as the interface to the TIBER Test Manager. The members of the White Team are the only people within the entity to be informed about the planned test; the work units in charge of combatting cyber attacks (Blue Team) must remain unaware of the test, as the informative value of the test would otherwise be significantly limited. In this phase, the White Team determines the scope and objectives of the test, which must then be approved by the entity's board and passed on to the TIBER Test Manager and BaFin. The test should focus on the critical systems and processes.

It is also during this phase that the White Team carries out a risk assessment and establishes the risk management controls necessary for the TIBER-DE test. Active and robust risk management is a major component of a TIBER-DE test and lies within the entity's responsibility. This is particularly important because such testing examines the entity's critical live production systems, which means that there is a risk of disruptions or outages in these systems.

Finally, the entity commissions the service providers – the Threat Intelligence Team (TIT) and the Red Team (RT) which are the key actors in a TIBER test. For the purposes of TIBER-EU, the Red Team and the Threat Intelligence Team must be independent, external service providers that meet the requirements of the Services Procurement Guidelines published for TIBER-EU. In this respect, TIBER-EU[11] explicitly calls for the deployment of external red teams, as they might use alternative approaches, tools or expertise in conducting the test that internal testers would possibly overlook or neglect. Internal experts can support the external testers to a reasonable extent.

Since the external service providers are given in-depth knowledge of the entity's cyber security during testing and the test is conducted on the entity's live production systems, it is important to select such service providers with great care to avoid potential risks.

10 TIBER-EU White Team Guidance – The roles and responsibilities of the White Team in a Threat Intelligence-based Ethical Red Teaming test, December 2018, https://www.ecb.europa.eu/pub/pdf/other/ecb.tibereu.en.pdf, retrieved on 3 December 2019.

11 TIBER-EU FRAMEWORK – Services Procurement Guidelines, August 2018, https://www.ecb.europa.eu/pub/pdf/other/ecb.1808tiber_eu_framework.en.pdf, retrieved on 3 December 2019.

Testing phase

Before the actual testing phase begins, the Threat Intelligence Team prepares the Targeted Threat Intelligence Report for the respective entity. This report – based on the generic threat landscape, where applicable – describes the entity-specific threat landscape. It addresses possible attack scenarios and vulnerabilities as well as other useful information about the entity. The Targeted Threat Intelligence Report is made available to the parties concerned within the entity, the TIBER Test Manager and the Red Team and is discussed with them. Drawing on the approaches taken with other national implementations, additional possible measures for the quality assurance and enhancement of the targeted threat intelligence process are being reviewed for the purpose of TIBER-DE.

After deriving specific attack scenarios from the Targeted Threat Intelligence Report and with the defined objectives in mind, the Red Team carries out the attacks on the entity's critical systems, organisational structures and processes. If the Red Team is unable to progress to the next stage in its attacks, the TIBER-EU Framework allows for the White Team to provide the Red Team with expert assistance. This is to ensure that, if possible, all the systems important for achieving the objectives are tested.

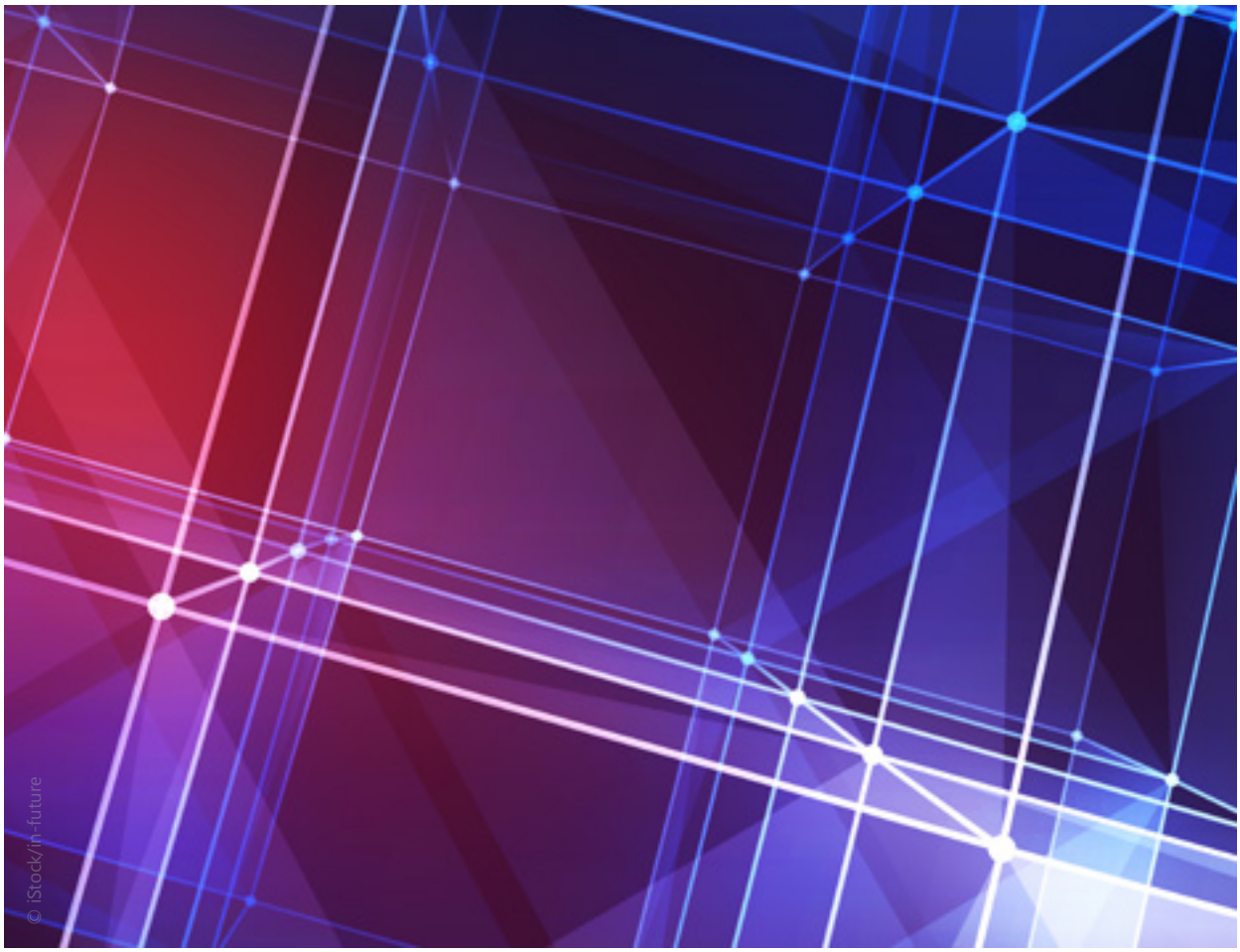
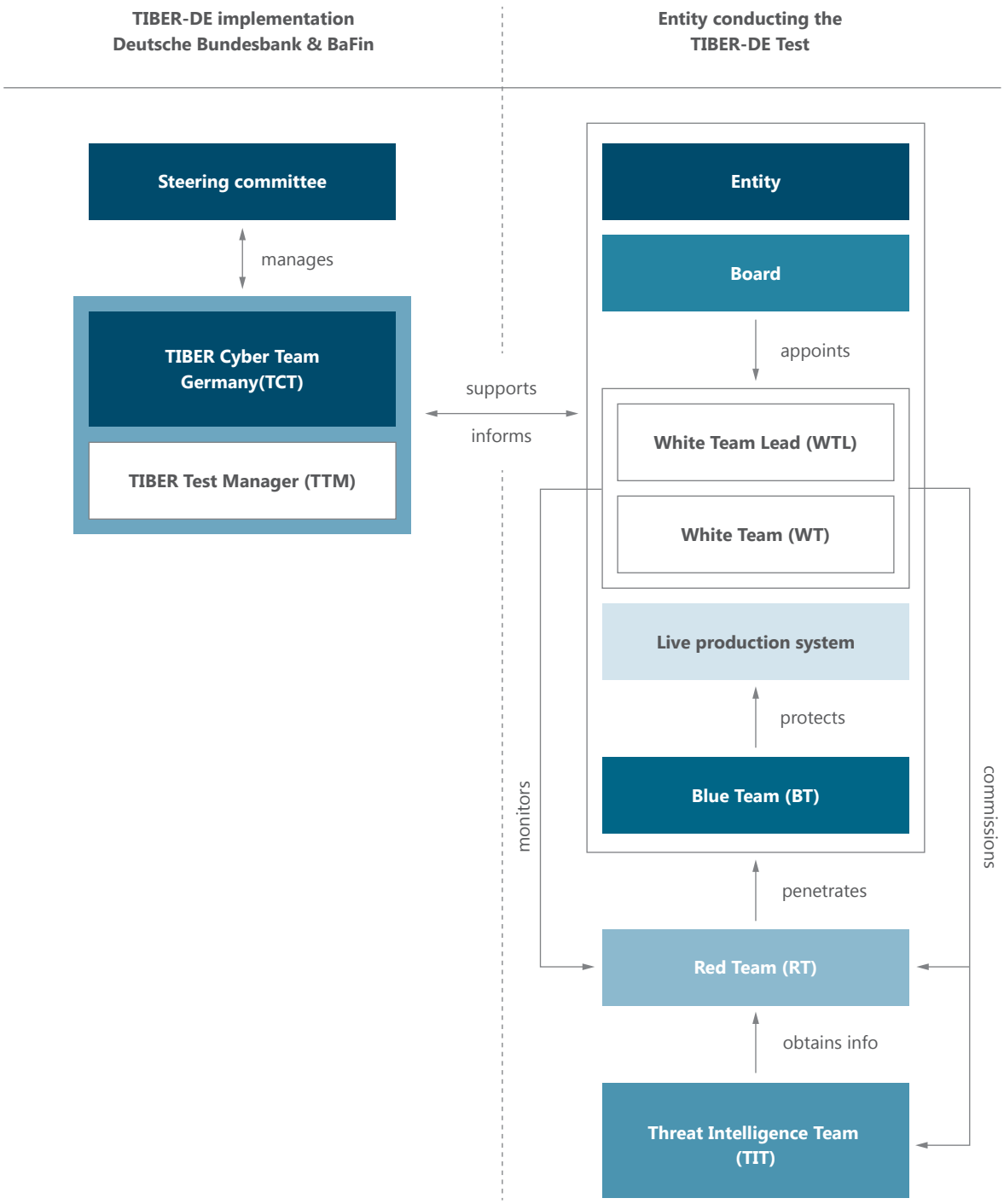


Figure 2: Actors and roles in the TIBER-DE implementation and the TIBER-DE tests



Source: Deutsche Bundesbank

The risk management specifically set up by the entity prior to the test must ensure during testing that the risk mitigation measures and monitoring tools are effective. For this reason, the Red Team must closely involve the White Team in the test process. The TIBER Test Manager must also be informed about the progress of the test on a regular basis (at least weekly).

Closure phase

In the closure phase of the TIBER-DE test, the results are analysed, follow-up measures are agreed and all the findings are communicated to the relevant parties identified in the TIBER-DE framework.

At the beginning of this final phase of the TIBER-DE test, a 360-degree feedback meeting is held with all the participants, including the TIBER Test Manager; the purpose of the meeting is to analyse the test findings. Furthermore, the Red Team prepares a Test Summary Report showing the procedure and the results. If necessary, the report should also include detailed information on how defence mechanisms (e.g. relating to physical or technical safeguards, company policies and business processes, employee training and raising employee awareness) can be improved in future. This report is then provided to the TIBER Test Manager.

As part of the strategic development of TIBER-DE, the possibility of establishing an optional "Purple Team" in the closure phase of a test is currently being discussed. This means bringing the Blue Team and the Red Team into dialogue to discuss attacks, other attack possibilities and defence measures envisaged by the entity for such cases. This exchange could make a significant contribution to the lessons learned from the TIBER-DE test.

Finally the entity drafts a Remediation Plan for mitigating the vulnerabilities identified by the test.

The findings of the TIBER-DE test are of major importance for both the entities' technology experts and the management level. Not only will they make it possible to detect vulnerabilities in the area of cyber security and remedy them adequately – they will also help to visualise the impact of cyber attacks and their specific implications (such as the leakage of sensitive information, data changes).

4 Conclusion

TIBER-DE tests will enable entities to review their cyber resilience under realistic conditions and visualise the impact of possible cyber attacks. Once the TIBER-EU Framework has been implemented in Germany, entities will have the opportunity to undergo threat-led ethical penetration testing. The requirements of the framework ensure that the quality of the tests will be high and that they can be mutually recognised across countries. A collaborative approach, with the entities and authorities involved working closely together, is expected to enhance cyber resilience in the entire financial sector and thus ensure an adequate response to the risks inherent in digitalisation.

“The danger is real. And it is growing.”

Interview with

Raimund Röseler
Chief Executive Director Banking Supervision,
Federal Financial Supervisory Authority (BaFin)

Lots of data and lots of money make the financial sector a popular target for cyber criminals. In Raimund Röseler’s opinion, the coronavirus pandemic could make things even worse. Nevertheless, BaFin’s Chief Executive Director Banking Supervision also knows that most IT-related losses and damage are still caused accidentally – at IT services providers or internally, through faulty hardware or an organisation’s own staff. In fact, the latter are particularly error-prone during the coronavirus crisis, because working conditions and workflows are no longer what they used to be.

In this interview with BaFinPerspectives, Röseler explains the steps that need to be taken if banks or other payment service providers are hit by cyber attacks or internal IT disruptions, and the areas in which the regulatory framework still needs to be improved.

Mr Röseler, how does BaFin find out about cyber attacks and IT disruptions in the first place?
Since 2018, payment service providers such as banks have been required to report major cyber incidents – or to be more precise: major operational or security incidents (see the infobox on page 57) – to us. These cover external attacks and sabotage by employees, but also unintentional internal disruptions.

Critical infrastructure operators throughout the financial sector are also subject to a notification requirement. In this case, though, the addressee is the Federal Office for Information Security (*Bundesamt für Sicherheit in der Informationstechnik* – BSI).[1] However, the BSI forwards us the notifications if they relate to organisations that we supervise. This keeps us in the picture as well.

But what is missing are the insurers and the securities market.
You are right. There are no all-encompassing notification requirements in insurance and securities supervision. This means that there are still some gaps in information coverage.[2] Luckily, though, we are now seeing initial attempts to eliminate this problem and to harmonise reporting requirements. There is also a move to potentially simplify existing obligations at the same time. The European Commission held an initial consultation on this issue in December 2019 in the form of a survey[3].

1 See page 62 et seq.
2 See page 69 et seq.
3 European Commission, Digital Operational Resilience Framework for financial services: Making the EU financial sector more secure, https://ec.europa.eu/info/sites/info/files/business_economy_euro/banking_and_finance/documents/2019-financial-services-digital-resilience-consultation-document_en.pdf, retrieved on 7 May 2020.

At a glance

Cyber incident

A cyber event is an incident caused unintentionally or by malicious activity that

- jeopardizes the cyber security of an information system or the security of the information which the system processes; or
- violates the security policies, security procedures or acceptable use policies.[4]

Malicious cyber incidents can be external attacks but also cases of sabotage within organisations. These must be distinguished from internal disruptions unintentionally caused by staff. Such internal disruptions are also included in the term "cyber incidents".

The German Payment Services Supervision Act (*Zahlungsdiensteaufsichtsgesetz* – ZAG) does not use the term "cyber incidents", but instead talks about "major operational or security incidents". In principle, this means the same thing, although the term "cyber incident" is not limited to payment service providers but applies to the entire financial sector.

Notification requirement

Section 54 (1) of the ZAG requires that:

"Payment service providers must notify BaFin without undue delay of any major operational or security incidents. BaFin must provide the relevant details of the incident to the European Banking Authority and the European Central Bank without undue delay upon receipt of a notification. BaFin must assess the relevance of the incident to other authorities in Germany whose operational responsibility is affected and must notify them accordingly."

Let us look at the banks and other payment service providers. These have had to report major incidents since 2018. Can you give us some figures – including on losses and damage?

Yes and no. To date, 680 major cases have been reported to us.[5] Losses and damage are hard to quantify. Examples of aspects that would have to be taken into account include financial losses suffered by the institutions concerned, reputational damage, customer losses and – last but not least – potential damage to financial stability. You cannot automatically say that because it is a major incident the losses and damage are extremely severe. Other criteria play a role in this, including the institution's size, the duration of the incident and how significant the affected systems and services are.

4 See Financial Stability Board (FSB), Cyber lexicon, page 9, https://www.fsb.org/wp-content/uploads/P121118-1.pdf, accessed on 21 April 2020.

5 As at 20 April 2020.

Were these major incidents external attacks?
Only a small number of them were – 14 out of the 680 cases reported, to be precise. A large majority of the incidents were caused by internal factors such as human error and faulty processes or IT systems.

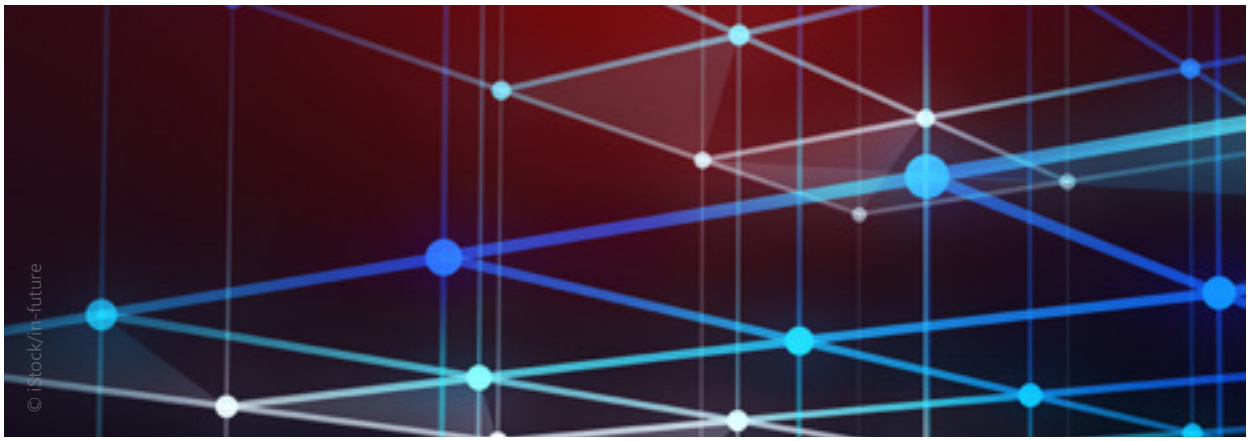
Has the number of major incidents reported gone up since the start of the coronavirus pandemic?
We cannot see any significant increase yet in the major incidents that are reported to us. However, it may well be that this will be the case at some point. A very large number of people are now working from home, workflows are increasingly being digitalised, and capacity utilisation levels for IT infrastructures are high. In addition, the coronavirus crisis seems to be leading to a general rise in cyber activity, including in the financial sector. For example, in April a US IT service provider was the victim of a cyber ransom attack which led to data being encrypted. This impacted a large number of US banks.

Have payment service providers directly affected by cyber attacks been able to withstand these attacks successfully so far?
Yes. German financial services providers that have fallen victim to cyber attacks have coped well. This is good news, of course. However, what is important to us is that institutions constantly review how they communicate during crises. News of cyber incidents spread like wildfire, especially on social media. Often such reports are more or less unfounded rumours. They can do severe damage to the institutions concerned.

And other than that payment service providers do not have any weaknesses when it comes to crisis management?
I would not go so far as to say that, but it is true that the institutions' weaknesses tend to lie elsewhere. Our on-site IT audit campaign at small and medium-sized banks[6] in 2019 revealed that the most significant deficits were in the areas of information risk management and authorisation management. There were also significant deficits in the fields of information security management and outsourcing management.

Going back to crisis management: did BaFin contribute to the organisations' relatively strong showing?
Yes it did in my opinion. For example, we require banks to have contingency plans ready for use in case of emergencies. They also have to test these regularly. Good crisis management is the crucial factor here. There have not been many cyber attacks yet, and the banks have weathered them well. But the danger is real. And it is growing. Our Supervisory Requirements for IT in Financial Institutions (*Bankaufsichtliche Anforderungen an die IT* – BAIT) spell out in detail what crisis management must look like to function successfully. The requirements specified in our VAIT and KAIT (see the infobox on page 59) are equally high.

6 Less Significant Institutions (LSIs).



At a glance

A three-stage approach to enhancing IT security

BaFin has developed a three-stage programme for its IT supervisory duties.

Stage One comprises a suite of three circulars setting out comparable IT requirements for organisations in the various supervisory areas: the Supervisory Requirements for IT in Financial Institutions (*Bankaufsichtliche Anforderungen an die IT* – BAIT)[7], the Supervisory Requirements for IT in Insurance Undertakings (*Versicherungsaufsichtliche Anforderungen an die IT* – VAIT)[8] and the Supervisory Requirements for IT in Asset Management Companies (*Kapitalverwaltungsaufsichtliche Anforderungen an die IT* – KAIT)[9].

In the BAIT, VAIT and KAIT, BaFin spells out in detail the requirements that organisations have to meet in the areas of IT governance and information security. The BAIT flesh out section 25a of the German Banking Act (*Kreditwesengesetz* – KWG), while the VAIT provide greater detail on section 23 of the German Insurance Supervision Act (*Versicherungsaufsichtsgesetz* – VAG) and the KAIT do the same for section 28 of the German Investment Code (*Kapitalanlagegesetzbuch* – KAGB). All three of the BaFin circulars make clear that senior management is responsible for IT security. One of the goals of these circulars is therefore to raise boardroom awareness of IT risks, including the risks that may arise when IT services are outsourced or purchased externally.

In addition, BaFin has published guidance[10] on outsourcing to cloud service providers in order to minimise uncertainty when outsourcing and hiving off services to such entities.

The aim in **Stage Two** is to audit compliance with these circulars on-site. In addition, Stage Two aims to further enhance banks' resilience to cyber attacks and their ability to ensure the continuity of their operations. BaFin does this by focusing more closely on the effectiveness of existing security measures. Stage Two also includes red team tests[11] – a sort of cyber stress tests for the German financial sector.

Stage Three is about improving crisis management: both the institutions concerned and BaFin must be prepared to deal with cyber attacks or IT-related operational incidents at all times. BaFin has therefore expanded the BAIT to include a module on contingency management, including contingency tests. In addition, cyber exercises are held in which all relevant players practice cooperating in crises – both at a national and at an international level. The planned "cyber crisis plan" (see the infobox on page 60) also forms part of Stage Three.

What can BaFin do if there is a cyber incident at a bank, for example?
There are a number of different ways in which we can take action. For example, we ensure that the organisation concerned informs us in depth of what is going on, and that it continues to keep us updated. We can publish press releases to ensure that the incident is treated in an objective manner – including on social media. We also support information-sharing between the affected parties so as to increase the speed with which incidents can be resolved.

Another extremely important point is that we work together closely with the other institutions involved

7 www.bafin.de/dok/10445406.
8 www.bafin.de/dok/11733690.
9 www.bafin.de/dok/14115822.
10 https://www.bafin.de/dok/13003422.
11 See also page 50 et seq.

– such as the BSI, the European Central Bank, the Deutsche Bundesbank and the Federal Ministry of Finance (*Bundesfinanzministerium*). This is because we also aim to prevent any damage to financial stability. In the case of major incidents, we also inform the National Cyberdefence Centre (*Nationales Cyber-Abwehrzentrum* – NCAZ). We can also involve law enforcement agencies. Or our colleagues in the states belonging to the G7 – although we would only do this if a cyber incident develops international dimensions. This network of different institutions is extremely important for us.

Does BaFin help affected organisations pick up the pieces?
No, we are not there to clear up the mess at a technical level. That is not our job, and nor do we have the necessary expertise. The organisations themselves or specialised service providers do this. Besides, every financial services provider is different from a technical perspective. That means they generally know best how to tackle the problem.

Our role is a different one: we want to help mitigate the impact of cyber incidents. We do this in the ways I have just mentioned, among other things. By bringing everyone affected together, providing the market with objective information, and so on.

We talked earlier about an IT service provider in the USA. Can BaFin take action when the problem is not at a bank or insurer but at their IT service provider?
That is an important point. And there is no single answer yet in that area either. As insurance supervisors, we have direct powers over third-party service providers. As banking supervisors, we also audit third-party providers but are not quite in such a strong position. We are currently considering whether to change and harmonise the overall framework in Germany and if so, how. At a general level, we need to ask ourselves how we can suitably address the significance, which in some cases may be systemic, of large third-party providers in the area of IT to which many different banks and insurers outsource operations. However, this is not just a question that affects Germany – Brussels should be asking this, too.

Let us assume that a number of banks are affected – or even a mixture of banks and insurers or other financial services providers. Would BaFin be able to cope?
This situation has never happened yet, but it would be an example of a cyber crisis and would therefore be covered by our cyber crisis plan. We are planning to roll this out BaFin-wide and are currently in the fine-tuning phase.

In a cyber crisis (see the infobox) we are also fighting against the clock. We have to be able to respond and take the right decisions within a short period of time. This means that we need to be able to communicate with all those involved right away and agree on the course of action extremely quickly and without difficulty. Something like this cannot be left to chance; we need to get everything right first time. This is why we have developed our cyber crisis plan. I think it puts us in a strong position. As I said, we have not been exposed to a cyber crisis yet and so have not needed to get the plan out so far. But we have successfully tested it several times – including in front of critical external observers.

Defintion

What is a cyber crisis?

The cyber crisis plan defines a cyber crisis as a cyber incident (see the infobox on page 57) that impacts the functions performed by one or more supervised undertakings

- which if not performed would endanger the real economy or the financial system, or
- whose sudden failure would probably have a material impact on third parties or would lead to contagion, or could undermine general trust among market participants.

Let us take that thought a bit further: how would BaFin react if a cyber crisis were to turn into what we might call a conventional crisis? A liquidity crisis, for example.
Such a situation cannot be ruled out and we have included such scenarios in our cyber crisis plan. In addition, BaFin already has contingency plans for these "conventional" crises – and has had them for a long time. Now we are dovetailing our cyber crisis plan with them. Our goal is to be able to take decisions and action immediately in such cases. There has to be transparency as to who informs whom about what, who takes what decisions and so on. Here, too, we are in a good position. But I would be happier if it never got to that.

I cannot say it often enough: we need smooth crisis management – both at the level of the organisations and at BaFin. At the same time, we also need strong defences. This is why we have drawn up strict requirements for both of these – crisis management and defence – in our BAIT, VAIT and KAIT circulars (see the infobox on page 59).

A cyber crisis could lead to a conventional crisis and turn into a systemic crisis: in February 2020, the European Systemic Risk Board classified cyber risks as a potential risk for the financial system as a whole.[12] And in 2019, the German Financial Stability Committee already identified cyber risks as systemic risks for Germany. What could a systemic incident look like?
I would define a systemic incident as one in which critical services provided by the financial sector are no longer available due to an IT disruption. This could result from either a cyber attack or an internal disruption. Imagine a situation in which the cards issued by a major bank no longer work because something was configured wrongly by mistake. This would mean that this bank's clients would no longer be solvent from one moment to the other. Oh joy. Think about if you had just filled up with petrol or were standing in line at the supermarket to pay for a really big shop. Or if you are a service provider and urgently need to order merchandise.

If something like that happens, the critical question is for how long the disruption goes on. If it lasts for a long time or if we are already in the middle of a crisis anyway – you only have to think of the coronavirus pandemic – this could seriously impact clients. In such a case we might be forced to take action.

The situation could also get worse if clients of other banks were to get nervous and take money out because they are afraid they might not be able to do so later. In that case it would not take long for a run on the banks to set in – something we all fear. And that in turn could lead to liquidity squeezes at banks that did not actually have anything to do with the IT incident.

Have there already been any such systemic incidents?
We have already had incidents in which critical functions at a major bank or an entire banking network were out of action. However, these only last for a very short period of time and the institutions involved managed to combat them in time and contain their effects early on. What's more, the information channels that I just described worked extremely well.

Thank you very much for talking to us, Mr Röseler.

Ursula Mayer-Wanders (Directorate K) with the assistance of Theresa Nabel and Dr Sebastian Silberg (both Directorate IT Supervision).

12 ESRB press release, ESRB publishes report on systemic cyberattacks, https://www.esrb.europa.eu/news/pr/date/2020/html/esrb.pr200219~61abad5f20.en.html, retrieved on 30 April 2020.

Supervising critical infrastructure in the finance sector – an overview of the status quo

Author

Dr. Wolfgang Finkler
Section WG 14 - CI Sectors Finance and Insurance, Information Technology and Telecommunications, and Digital Services, Federal Office for Information Security (BSI)

1 Introduction

Germany's 2015 IT Security Act (*IT-Sicherheitsgesetz* – IT-SiG) laid the foundations for overseeing the IT security of critical infrastructure operators' systems. The term "critical infrastructure" as defined in the Act also includes systems used in the finance and insurance sector. Such installations are already regulated in part by the German Banking Act (*Kreditwesengesetz* – KWG), the German Payment Services Supervision Act (*Zahlungsdiensteaufsichtsgesetz* – ZAG) and the German Insurance Supervision Act (*Versicherungsaufsichtsgesetz* – VAG).

2 Overview of regulated supervised critical infrastructure entities in the finance sector

The entry into force of the First Regulation Amending the Regulation on the Identification of Critical Infrastructure (*BSI-Kritisverordnung* – BSI-KritisV),[1] which was issued by the Federal Ministry of the Interior (*Bundesministerium des Innern* – BMI) in June 2017, extended the identification of critical infrastructures to the finance and insurance sector. Five critical services were specified together with categories of systems, measurement criteria and threshold values that enterprises and institutions can use themselves to determine whether they count as critical infrastructure operators. For example, the "conventional payment systems" critical service has "account management system" as a system category with "number of service-related transactions per year" as the measurement criterion and a threshold value of 100 million. This means that all account management systems that process more than 100 million transactions per year are classed as critical infrastructure as defined by the Act and must be protected accordingly.

The following article focuses solely on three critical services: cash supply, card-based payment transactions and conventional payment transactions. In this context, critical infrastructure operators are defined as enterprises that, "having regard to the facts of the case, have control over the system" used to provide the critical service, i.e. the enterprise that is actually in possession of it.[2]

In the meantime, a group of around 90 enterprises in the finance sector have identified themselves as critical infrastructure operators and registered with the Federal Office for Information Security (*Bundesamt für Sicherheit in der Informationstechnik* – BSI), and are now overseen by it. This group includes banks and payment services providers that are supervised by the Federal Financial Supervisory Authority (*Bundesanstalt für Finanzdienstleistungsaufsicht* – BaFin) under section 1 (1) of the KWG or section 1 (1) of the ZAG, or that are supervised by the European Central Bank (ECB) under the SSM Regulation.[3] In addition, some IT service providers perform payment services for banks under section 25b of the KWG or section 20 (1) of the ZAG and therefore are indirectly supervised by BaFin. Finally, the group also includes entities that perform payment services in the payments value chain but are not indirectly supervised by BaFin. These are supervised solely by the BSI.

1 Federal Gazette (Bundesgesetzblatt) Part I No. 40, 29 June 2017, page 1903 et seq.

2 Federal Gazette (Bundesgesetzblatt) Part I No. 40, 29 June 2017, page 1904, section 7 (8).

3 Regulation (EU) No. 1024/2013, Official Journal of the European Union L 287/63, 29 October 2013. "SSM" stands for the Single Supervisory Mechanism, of which BaFin is also a part. Significant Institutions (SIs) are directly supervised by the ECB under the SSM. Less Significant Institutions (LSIs) are supervised at national level.

3 Support for critical infrastructure operators

How do the supervisory authorities support critical infrastructure operators preparing to meet the statutory requirements set out in section 8a of the BSIG? We shall start by looking at the offerings and ways adopted by critical infrastructure operators in the finance sector to meet their preventive duties under section 8a (1) of the German Act on the Federal Office for Information Security (*Gesetz über das Bundesamt für Sicherheit in der Informationstechnik* – BSIG).

Section 8a (1) of the BSIG requires "critical infrastructure operators, at the latest within two years of the statutory order in accordance with section 10 (1) coming into force, to take appropriate organisational and technical precautions to avoid malfunctions in respect of the availability, integrity, authenticity or confidentiality of those of their IT systems, components or processes that are key to the functioning of the critical infrastructures operated by them. The state of the art is to be observed during this process. Organisational and technical precautions are taken to be appropriate if the effort needed to take them is not disproportionate to the consequences of a failure or an impairment of the critical infrastructure concerned."

B3S – Sector-specific security standards

As is the case for all sectors and industries, critical infrastructure operators and their industry associations can develop sector-specific security standards (*branchenspezifische Sicherheitsstandards* – B3S) designed to ensure the efficient formulation of typical requirements and measures for prevention complying with the state of the art, and can submit them to the BSI, which will then evaluate their suitability. This does justice to the fact that the CI sectors may exhibit a certain heterogeneity with respect to the industries involved and the technology deployed in individual cases. Following successful review, the suitability of B3Ss that have been submitted is determined in consultation with the Federal Office of Civil Protection and Disaster Assistance (*Bundesamt für Bevölkerungsschutz und Katastrophenhilfe* – BBK) and in agreement with the competent federal supervisory authority (generally BaFin in the case of the finance sector), or in the case of the social insurance institutions with the Federal Office for Social Security (*Bundesamt für Soziale Sicherung* – BAS).

Typically, B3Ss are developed in industry working groups under the UP KRITIS[4] public-private partnership. The BSI has published an Orientation Guide on the desired contents of, and requirements to be met by, B3Ss to aid in their preparation.[5] A number of relevant standards can be used as starting points both with respect to requirements and for more concrete instructions as to the state of the art; these include but are not limited to the ISO/IEC 27000 family of information security standards, the BSI's *IT-Grundschutz* (baseline protection) methodology, the PCI DSS standard, BSI Standard 100-4 and ISO 22301 Business Continuity Management. Their goal is to ensure that operators take security and business continuity aspects into account.

This approach was adopted for some of the more technology-dominated critical infrastructure systems in the area of card-based payment transactions – including in the case of the German Banking Industry Committee (GBIC)'s network operators for the areas of "Integration with authorisation systems from the perspective of the terminal device operator" and "Introduction of transactions into the payment system" formulated in the BSI-KritisV. The BSI determined the suitability of a B3S that refers heavily to elements of the PCI DSS[6] standard by declaring these to be key to the state of the art and adding supplementary requirements. This means that the long list of PCI DSS requirements that critical infrastructure operators may be able to already document as having been met during certification under PCI DSS, can now also be included on the basis of

4 The UP KRITIS is a public-private partnership between critical infrastructure (CI – in German KRITIS) operators, their industry associations and the competent public authorities.

5 https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/IT-SiG/b3s_Orientierungshilfe_1_0_en.pdf?__blob=publicationFile&v=2, retrieved on 16 March 2020.

6 Payment Card Industry (PCI) Data Security Standard, Requirements and Security Assessment Procedures, Version 3.2.1, May 2018, https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2-1.pdf

this sector-specific security standard in the verification that is submitted to the BSI. In addition, the operators already have to meet security requirements to obtain authorisation as network operators for the GBIC's electronic cash system.

Reducing the additional burden as far as possible

The starting point for critical services in the area of payment transactions in the finance sector is the recognition that a number of institutions that have now become critical infrastructure operators and must meet the associated statutory requirements are already subject to the institutionalised supervision of credit institutions by BaFin and the Deutsche Bundesbank at the federal level, or to European banking supervision under the SSM. The Supervisory Requirements for IT in Financial Institutions (*Bankaufsichtliche Anforderungen an die IT* – BAIT)[7] formulated in BaFin circular 10/2017, which interpret the standards applicable to the banking sector in relation to the requirements for a proper IT business organisation, already apply in these cases. Writing jointly,[8] the presidents of the BSI and BaFin have informed the sector the objective is to minimise as far as legally acceptable the additional material burden on institutions that now also qualify as CI operators. After this, BaFin published an update to the BAIT[9] in the form of the CI section, in cooperation with the BSI. This sets out additional requirements to be met by institutions that are also CI operators. In addition, item 61 of the BAIT in the version dated 14 September 2018 permits the verification required to be submitted to the BSI to be obtained from the auditor of the annual financial statements in the course of the audit by enhancing the audit scope.

Well before the update to the BAIT was introduced, the BSI had specified on its website[10] the general conditions it considers necessary for permitting critical infrastructure operators that are already ISO 27001-certified to use such certifications in their verification that they have met the requirements of section 8a of the BSIG. By doing so, the BSI created the basis for implementing the provisions of the KritisV as simply as possible. The general conditions described by the BSI also address the questions of the scope of the certifications and the inclusion of the CI protection objectives,[11] which are also formulated in item 57 of the BAIT in the version dated 14 September 2018. The core concern of the CI protection objectives is to guarantee security of supply for the population when addressing information security risks. In addition, they describe how to deal appropriately with risks. Among other things, banks should state that they have implemented measures. It is not enough to report planned measures.

7 Circular 10/2017 (BA) – Supervisory Requirements for IT in Financial Institutions (BAIT).

8 BaFin, Bankaufsichtliche Anforderungen an die IT Kritischer Infrastrukturen (Supervisory Requirements for IT in Financial Institutions for Operators of Critical Infrastructures), www.bafin.de/dok/11327090, retrieved on 16 March 2020.

9 BaFin, Kritische Infrastrukturen: BaFin ergänzt BAIT um Kritis-Modul (Critical infrastructure: BaFin updates BAIT to include CI section), www.bafin.de/dok/11486774, retrieved on 16 March 2020.

10 BSI FAQs, https://www.bsi.bund.de/DE/Themen/KRITIS/IT-SiG/FAQ/FAQ_8aBSIG_ISO27001/faq_bsi_8a_ISO27001_node.html

11 https://www.bsi.bund.de/DE/Themen/KRITIS/IT-SiG/Was_tun/Stand_der_Technik/Orientierungshilfe/Orientierungshilfe_node.html, retrieved on 16 March 2020.

4 Lessons learned to date from the verifications submitted by critical infrastructure operators

The verifications that had to be submitted in June 2019 under section 8a (3) of the BSIG and were submitted to the BSI showed that, as was to be expected, the operators adopted very different approaches to meeting the requirements of section 8a (1) of the BSIG with respect to the alternatives set out in the previous section – use of a sector-specific security standard (B3S), of the BAIT CI section or of certifications in a supplementary audit.

The audit effort data of which the BSI was informed vary considerably and ranged from relatively short supplementary audits including existing certifications of information security management systems down to lengthy independent audits. In addition, some operators are only responsible for a small number of critical infrastructure systems, whereas other operate more than a dozen such systems. This, too, leads to varying levels of audit effort. The audits were required to examine the entire scope of the critical infrastructure in each case.

Quite often, the auditors of the CI operators developed an individual basis for the audit themselves; this was typically derived from the topics contained in the B3S Orientation Guide.

Many of the network operators authorised by the German Banking Industry Committee (GBIC) used the B3S mentioned earlier as the basis for the audit. By contrast, verification reviews using the supplementary CI section of the BAIT were only rarely performed at credit institutions.

Multistage procedure at the BSI

Once submitted to the BSI, the verifications undergo a multistage review procedure. In a first step, the BSI checks whether the verification documents are complete. After this, a plausibility check at the least is performed. In general, additional communication with the critical infrastructure operators is required at both stages, since the verifications mostly contain deficits and therefore additional requests have to be made for information or documents. For example, in a number of verification reviews the BSI had to ask whether the aspects relating to the special treatment of measures taken to protect critical infrastructure had been included in the audits. After this, the BSI requested corresponding updates to the security guidelines from the operators.

Equally, the BSI had to make a number of follow-up inquiries and request additional documents from operators in order to be able to assess during its completeness and plausibility checks whether the scope of the audits at the critical infrastructure operators corresponded to the systems registered. Details of audit planning and implementation were also often missing.

The objective was for the auditing bodies commissioned by the critical infrastructure operators to confirm that the operators in each case have implemented appropriate measures that comply with the state of the art, as is required. In most cases, this was possible only to a limited extent, with substantial limitations in some cases. As prescribed, the operators documented the deficits found by submitting lists of deficiencies to the BSI, in which they informed it of security deficiencies (where were classified as “major” and/or “minor”). Where major security deficiencies were found, operators also had to submit an implementation plan for rectifying them, complete with the persons responsible, the measures to be taken and the target dates.

The auditing bodies identified security deficiencies at several critical infrastructure operators in the payment transactions area; in most cases, the numbers of such deficiencies were in single figures. This applies both to banks and to IT service providers in the payment transactions area. However, some of the supervised institutions have to rectify a relatively large number of such security deficiencies.

The large number of deficiencies identified in the finance sector was surprising, since many operators have already been subject to sector-specific audits for some time

and also furnish their clients with proof that they have functioning information security management systems in place – e.g. using existing ISO 27001 certifications. However, a current look at the deficiencies reveals that in many cases these relate to basic deficiencies in the implementation of information security management complying with section 8a (1) of the BSIG or in the documentation (such as are identified, for example, in the context of certification audits). These deficiencies do not as a rule represent a direct threat to the continuity of the technical and organisational operation of the critical infrastructure.

5 Next steps and conclusion

The BSI will closely track the measures intended to rectify security deficiencies of which it is informed by the operators, and will work to ensure they are implemented.

In individual cases, the BSI will, in agreement with the competent federal supervisory authority,[12] demand that security deficiencies be rectified; where necessary this may involve a different schedule and other sets of measures. Finally, the BSI may come to the conclusion in the course of its verification reviews that a detailed, in-depth audit of individual critical infrastructure operators is necessary, and may conduct such an audit.

Both the BSI and BaFin expressly welcome the in-depth, constructive dialogue between critical infrastructure operators and their associations on the one hand and the two supervisory authorities on the other. The verifications that have been submitted in fulfilment of the requirements of section 8a (1) of the BSIG show that the finance sector takes this issue seriously and that appropriate organisational and technical precautions have been taken to avoid malfunctions in respect of the availability, integrity, authenticity or confidentiality of IT systems, components or processes that are key to the functioning of the critical infrastructures being operated. However, they also show that the participants involved will need to continue this work in 2020 in order to remedy the deficiencies determined, as well as to enhance the resilience of the finance sector, for example in relation to forthcoming new digital transformation initiatives.

12 See section 8a (3), sentence 4 of the BSIG.

III

Insuring cyber risk

With a name like “sure”

Author

Dr. Frank Grund
Chief Executive Director of Insurance and Pension Funds Supervision, Federal Financial Supervisory Authority (BaFin)

1 Insurers – security ensured?

1.1 Insurers as targets for cyber attacks

Anyone with the word “sure” in their name ought to be utterly safe and secure, ready to face all the world’s evils – even those coming from cyber space.[1] This is not automatically the case, however. The fact is that insurers, similar to banks, are a favourite target for cyber attacks – and the reasons are obvious. They accept funds and move large sums of money. They also accumulate enormous quantities of highly sensitive data.

We can currently only speculate on how many attacks actually strike insurers. For one thing, insurers – unlike banks – have not been subject to any reporting requirements to date; this is a deficiency that urgently needs to be addressed. For another thing, we can assume that amongst the hackers are great masters of camouflage. We can thus hardly estimate with any reliability how many well-disguised cyber attacks go unnoticed.

In some cases, hackers camouflage themselves but not their attacks. They have a vested interest in making sure their work attracts attention – a characteristic feature of their criminal business idea. Take ransomware, for example: victims are absolutely supposed to find out that they have been attacked. After all, the point is to force them to pay a ransom for the return of their data.

The threat situation is serious. And because the adversaries are becoming more and more cunning, the gravity of the situation is even increasing. In its report “Cyber Risk for Insurers – Challenges and Opportunities”[2] issued in 2019, the European Insurance and Occupational Pensions Authority (EIOPA) uses strong words. According to the EIOPA findings, the increasing frequency and sophistication of cyber attacks is causing difficulties for insurers, and the intensified use of big data and cloud computing is making these undertakings susceptible to cyber threats. There is yet another aspect that must be taken into consideration, however: the imminent concentration risk.

1 This text is based on a speech given by the author at the 2020 annual conference of third-party liability insurers in Hamburg on 21 January 2020.

2 EIOPA, Cyber Risk for Insurers – Challenges and Opportunities, https://www.eiopa.europa.eu/sites/default/files/publications/reports/eiopa_cyber_risk_for_insurers_sept2019.pdf, retrieved on 27 March 2020.

1.2 Strengthening their own defences

In any case, the key question is this: is the industry as a whole arming itself adequately for the fight against cyber criminals? We should think so – after all, customer data are what the criminals are after, and customer data are the treasure of every insurer. One would expect each undertaking to be striving for a maximum level of IT security, in its own interest.

As can be anticipated, however, neither legislators nor supervisors intend to simply trust them to do so; there are thus regulatory requirements regarding IT security as well as supervisory circulars that expound on these requirements. We have consolidated these requirements for IT in our Supervisory Requirements for IT in Insurance Undertakings (*Versicherungsaufsichtliche Anforderungen an die IT* – VAIT[3]). The VAIT allow us to interpret the provisions of the German Insurance Supervision Act (*Versicherungsaufsichtsgesetz* – VAG) regarding the technical and organisational resources of the undertakings, in a binding, consistent manner. We want all undertakings and groups to know where they stand. This transparency is very important to us.

Planned attacks in the name of security

Under the VAIT, for example, we require information security officers to disclose the results of penetration tests in the status report they issue to their management board. In these tests, security specialists inspect the performance of an undertaking's IT security. Newer

3 Circular 10/2018 – Supervisory Requirements for IT in Insurance Undertakings (Versicherungsaufsichtliche Anforderungen an die IT – VAIT), www.bafin.de/dok/11733690.

versions of these tests – such as the TIBER tests – no longer focus predominantly on technical aspects but also take into account factors such as human error. In these tests, a "red team" attempts – like a real hacker – to break down an undertaking's physical, technical or organisational security mechanisms, aiming to achieve predefined objectives.

The strengths of the red team tests include their real-world approach, the depth of testing and the usability and visualisation of the results. These planned attacks illustrate the possible impact of a hacker attack – in a way that even those who are not IT security experts can get a clear idea of the threat landscape. The testing reveals specific vulnerabilities in the security measures that undertakings have in place, making it possible to mitigate them – preferably quickly. While these red team tests are not compulsory, it is in the undertakings' own interest to use them as a tool for improving their cyber security. It would make no sense if insurers, fearing supervisory sanctions in the event that their results were not particularly good, then chose to forego the tests. A red team test is not a matter of passing or failing. It is solely about optimising cyber security.

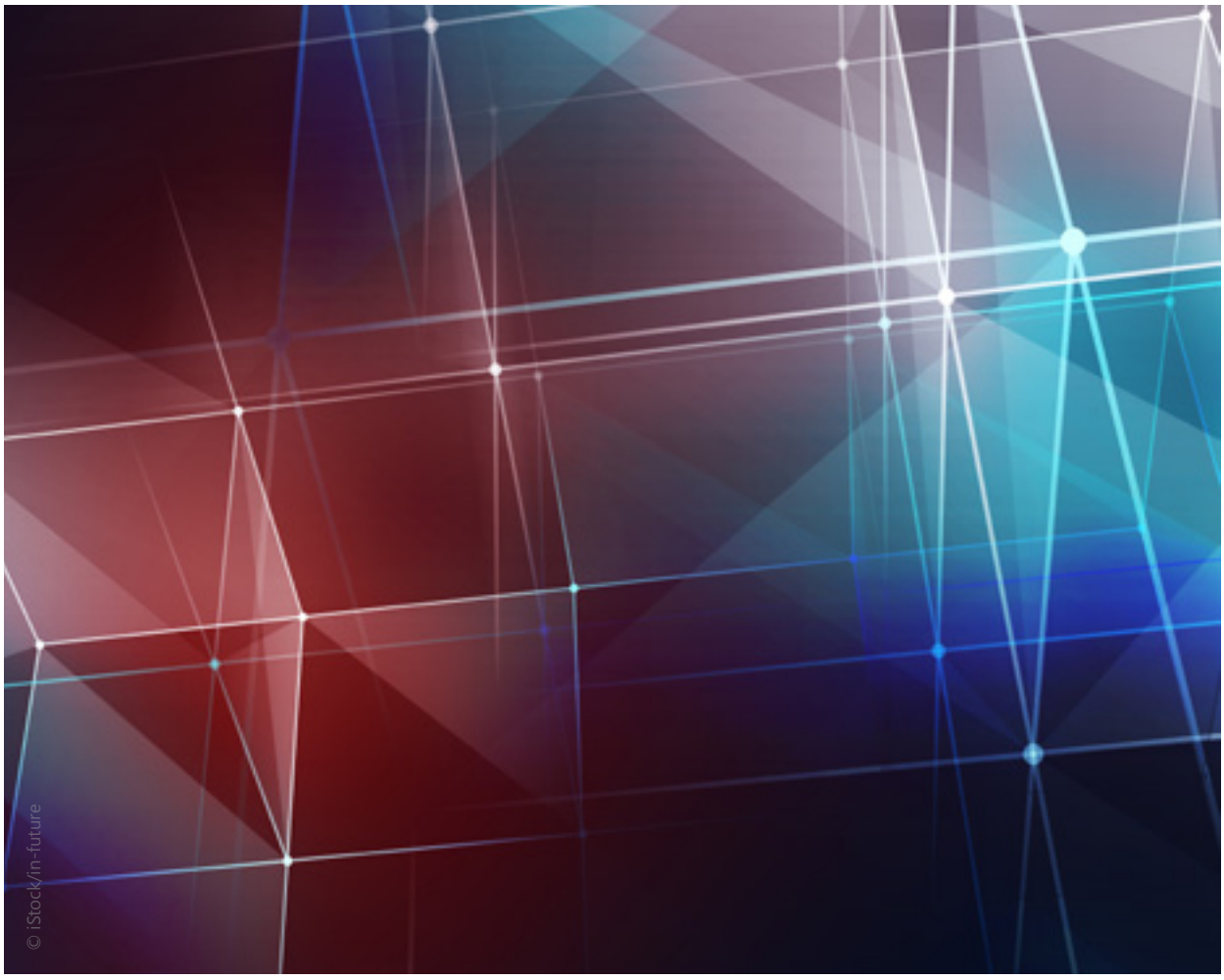
1.3 Achilles' heel

While BaFin does not conduct any penetration tests itself, it does carry out its own IT inspections. Sometimes these inspections give rise to findings that are surprising and not entirely positive. In inspections conducted in 2019 and 2020, we found that a number of insurers did not even have an information risk management system in place. They had not dealt systematically or adequately with material information risks, nor had they set up the process elements required under the VAIT: identification, assessment, monitoring and steering. These undertakings had an Achilles' heel, for without an effective information risk management system in place, cyber threats simply cannot be averted.

In terms of information security management, the situation was much the same. With some undertakings, we searched for it in vain, or what we found was inadequate. Our inspection teams asked for information

security policies or even merely for an information security officer; unfortunately, in a number of cases our search was unsuccessful. Furthermore, it is unacceptable that there should be some systems and applications that are not checked for security incidents at all. These are all glaring gaps.

In light of the overall situation, it is therefore not surprising that, in 2020, BaFin intends to focus on inspecting the IT and cyber security of insurance undertakings and other entities. To this end, BaFin plans in particular to monitor how the VAIT are being implemented in the industry. And though we are being compelled to adapt our priorities for 2020 in view of the rapid spread of the coronavirus, this does not mean we will be ignoring IT and cyber risks until a vaccine is found.



2 Third-party cyber incidents – a risk for insurers

2.1 Hidden risks

Beyond their own risk of falling victim to cyber attacks, insurers may also have to provide cover for third-party cyber incidents. The question whether an insurance undertaking must answer for third-party cyber risks does not depend on whether the policy is called "cyber insurance". Cyber risks can also lie dormant in insurance products which – unlike cyber insurance policies – do not explicitly address the extent to which cyber damage is covered. Such risks are called "hidden", "non-affirmative" or "silent" cyber risks. These hidden risks can be found lying in wait in many traditional contracts. Some of these contracts date back to a time where the topic of digitalisation/cyber risk had not yet begun to play a role, or at least a major role.

This is affecting property and casualty insurers in particular. Especially in their case, the tremendous increase in hacker attacks and other forms of cyber incidents could result in disruptive claims developments. Let us assume a hacker turns off the cooling system of an industrial plant, starting a fire. As fire is an insured risk, the property insurer would have to pay. The fact that this insurer, on concluding the contract back in analogue times, did not duly consider a scenario in which a hacker turns off the cooling system – and perhaps could not even have done so – makes no difference.

Non-affirmative cyber risks as a supervisory priority in 2019

Non-affirmative risks were a priority area for BaFin's Insurance Supervision in 2019. It was the supervisory authority's intention to ensure that insurers identified and assessed the non-affirmative cyber risks in their own insurance portfolio. While BaFin used its on-site inspections for this purpose, its supervisory interviews also addressed non-affirmative cyber risks.

In addition, BaFin surveyed 27 insurers and insurance groups regarding non-affirmative cyber risks, aiming to raise their awareness of the topic. To date, only two undertakings have indicated that damage had occurred due to non-affirmative cyber risks in their portfolios. It was striking that many insurers had never reported any such insured events up to that point. This could be interpreted to mean that the industry might have overestimated the threat of non-affirmative cyber risks to some extent. But our survey does not support an all-clear signal for all undertakings and every portfolio – this is also especially due to the fact that we still lack data. Approximately 50% of the survey participants said it was not easy to identify such cases in the first place.

The good news: in 2019, nearly all the insurers were taking non-affirmative risks into account in their risk management system and were monitoring claims development and market activities. The undertakings were also beginning to comb through their terms and conditions in search of silent risks. More substantial contract changes were not up for debate, however.

In summary, there are two messages for us here. First, insurance undertakings must intensify their efforts to investigate whether cyber incidents have been the cause of damage. Secondly, in light of potential non-affirmative cyber risks: insurers need to know their portfolio – or familiarise themselves with it as soon as possible!

2.2 Cyber insurance policies

Though products that call themselves "cyber insurance" and expressly insure cyber risks are relatively new, they have been around for several years. There is also no lack of model terms and conditions provided by the German Insurance Association (*Gesamtverband der deutschen Versicherungswirtschaft*). Cyber insurance policies are not traditional products. They are amongst the few innovations that digitalisation has generated in the insurance sector. They fill in a coverage gap between conventional insurance policies – for example, between business interruption insurance and liability insurance.

If hackers were to cripple an enterprise's IT system and steal its customer data, that enterprise would likely be barking up the wrong tree in expecting its business interruption and liability insurer to become involved. If no property damage or personal injury has occurred, many conventional policies issued in these segments cover neither the loss of earnings nor the claims of aggrieved third parties to whose accounts the hackers have helped themselves. Cyber insurance is intended to fill in these gaps.

Growth market

Cyber insurance is said to be a driver of growth. Auditing and management consultancy firm KPMG estimated the premium volumes for Germany at US$100 million in 2016.[4] This number is certain to be higher now but – in light of the 2.9 billion dollar US market – still modest. And yes, Europe still has a "cyber gap" that the market can fill – and filling this gap would enable the market to grow.

We should refrain from comparing apples and oranges, however. The German market is fundamentally different to the US market, which is strongly influenced by the concept of legal protection. Moreover, exaggerated aspirations for growth have never been beneficial. How reliable are projections if we do not even have any reliable actuals? Insurance undertakings are not obliged to provide BaFin with separate figures for cyber insurance policies – neither the German Insurance Reporting Regulation (*Versicherungsberichterstattungs-Verordnung*) nor Solvency II requires them to do so.

A report issued by EIOPA provides a number of findings regarding the European cyber market.[5] According to the information reported, insurers focus on commercial customers but are also taking individuals into consideration. The growing number of cyber incidents is raising awareness of the risk and thus driving demand for suitable insurance solutions. Another finding: insurers use qualitative models more frequently than quantitative models when pricing their insurance cover.

But besides the EIOPA report, it goes without saying that BaFin wishes to form its own impression of the German market for cyber insurance. In 2020 – according to our pre-pandemic planning – we intend to make the matter a priority and ask roughly 25 insurers a number of questions about the German cyber insurance market. We want to find out how many cyber insurance policies they have in their portfolios, what the premium volume is and how high the amount of damage is. But we also want to know whether the undertakings are in a position to price cyber risks properly. This is why we also intend to gain some insight into the underwriting and risk management at these insurers.

We will have to wait and see how far we get with this year's planning in view of the coronavirus crisis. But even in a time of pandemic, our appeal to insurers is still as familiar as it is urgent: be careful when underwriting cyber insurance policies, do not overestimate premium income and do not underestimate the accumulation risks!

4 KPMG, "Neues Denken, Neues Handeln – Insurance Thinking Ahead: Versicherungen im Zeitalter von Digitalisierung und Cyber (New ways of thinking, new ways of taking action – insurance thinking ahead: insurance in the age of digitalisation and cyber)", part B: Cyber, page 7, https://assets.kpmg/content/dam/kpmg/ch/pdf/neues-denken-neues-handeln-cyber-de.pdf, retrieved on 6 April 2020.

5 EIOPA, Understanding Cyber Insurance – A Structured Dialogue with Insurance Companies, https://www.eiopa.europa.eu/sites/default/files/publications/reports/eiopa_understanding_cyber_insurance.pdf, retrieved on 27 March 2020.

3 IT security at BaFin

BaFin has also set itself high standards in matters of IT security, for it is likewise a favourite target for hackers from cyber space. This is not surprising if we consider, for example, that BaFin has also been entrusted with tremendous amounts of highly sensitive data – including the data which insurers, bankers and other financial services providers are required to report to BaFin.

How does BaFin protect itself? Here are only a few examples: like all federal authorities, BaFin is required to implement the IT baseline protection recommendations issued by the Federal Office for Information Security (*Bundesamt für Sicherheit in der Informationstechnik*). Furthermore, BaFin adheres to the relevant DIN standards and the requirements of the European Central Bank (ECB). This stems from the fact that BaFin is part of the Single Supervisory Mechanism for the banks of the eurozone, led by the ECB.

BaFin is also protected by the central safeguards of Germany's public administration network. In addition, however, BaFin shields its network by taking measures itself. Its comprehensive security concept, updated on an ongoing basis, ensures that an attack on its IT infrastructure would be extremely difficult. While the authority does not make details of its concept public, for understandable reasons, this much can be said: all BaFin's points of access to the Internet are monitored at multiple levels. Files that are downloaded or received by e-mail are loaded into detonation chambers, where they are inspected in a separate environment. It goes without saying that certified firewalls and a wide range of anti-virus mechanisms are in place.

And, of course, BaFin attaches great importance to ensuring that all its employees deal responsibly with data and cyber security matters – for example, by raising employee awareness and providing training.

BaFin's ability to withstand cyber attacks is subjected to external testing on a regular basis. These tests, which are conducted by the Bundesrechnungshof, the ECB and auditors commissioned by BaFin itself, also include penetration tests. So far, the results have always confirmed BaFin's high level of security. And to date, as far as we can tell, none of the cyber attacks on BaFin have ever been successful. BaFin's Insurance Supervision Sector must likewise be sure of its security. But it must not feel too secure.

Cyber insurance becomes a crisis manager

Author

Dr. Christopher Lohmann
Chairman of the Board of *Gothaer Allgemeine AG*

with Melanie Schmitz, Frank Huy,
Oliver Schulze and Udo Wegerhoff,
Gothaer Allgemeine AG

1 Introduction

Today, almost every hotel uses an online booking system, most craftsmen maintain electronic customer files and it would be difficult to find a hospital that operates without digital patient files. These new technologies bring huge progress in all areas: they accelerate and simplify processes, and tasks can now be completed regardless of location or time. But they also make companies more vulnerable: those who rely on digitisation are potentially vulnerable to cyber attacks. Computer scientists are not the only ones that get sweaty palms at the thought of data theft, hacker attacks, identity theft, viruses, Trojans or even cyber blackmail. However, companies and consumers alike can protect themselves from the resulting consequences: with cyber policies.[1]

For insurers, the emerging market for cyber policies is at present probably the most exciting trend in the area of corporate insurance: the field is characterised by new products and a pool of German and Anglo-American competitors that is still relatively small, in addition to an ever-changing threat landscape and technological innovations. Complacency in this regard could leave insurers falling by the wayside in the long term.

The customer potential for cyber insurance is huge for providers. After all, there is no company today that could operate without an IT infrastructure – be it an industrial group or a medium-sized enterprise.

1 Regarding cyber policies see also page 73 et seq.

2 Fear of cyber attacks among SMEs

While large companies have the financial means to protect themselves against cyber attacks by applying modern solutions and hiring internal or external IT experts, the situation is often different for small and medium-sized enterprises (SMEs). Risk awareness, however, is also high among SMEs. This was shown by the SME study that Gothaer carried out in 2019[2] which included representatives of more than 1000 SMEs. Before the coronavirus crisis, the undisputed number one risk most feared by managers (43%) was a hacker attack, followed by burglary (36%) and business interruption (35%). The SME study also showed that almost one in five of the companies surveyed (17%) had suffered a cyber attack in the past. The number of undetected cases is likely to be significantly higher, since not every attack is noticed or reported. Most frequently affected were medium-sized companies with 200 to 500 employees, which in Germany are often technology leaders in their field and therefore a particularly attractive target for hackers.

The companies are well aware of the risk. They have good reason to fear the financial and legal consequences arising from cyber crime, which can be substantial and, in extreme cases, may even jeopardise the very existence of the company – for example in the case of long-term business interruptions. It is therefore all the more surprising that the percentage of SMEs that use cyber insurance to cover these risks is still relatively low. In Gothaer's SME study, only 13% of the respondents stated that they had taken out cyber insurance. At the same time, 23% of all SMEs surveyed stated that they were going to take out such cover in the next two years. However, 41% had no plans to do so, while 36% were undecided.

One thing is astonishing, though: virtually no company operates without having professional indemnity insurance: 88% of the SMEs surveyed stated that they had taken out such cover. But if a hacker attack is currently their biggest concern, as the study shows, why do so few companies take out cyber insurance to protect themselves against the financial and legal consequences of such an event?

2 Gothaer, KMU-Studie 2019, https://www.gothaer.de/ueber-uns/presse/publikationen/studien/kmu-studie-2019.htm, retrieved on 20 March 2020.

3 Damage caused without the attacker ever having set foot in the company

Gradually, however, companies are beginning to rethink. Gothaer's end-of-year figures for 2019 show a significant increase in cyber policies as compared to 2018. This growth is primarily driven by increased risk awareness among managers, but also by the fact that more and more focus is being placed on cyber insurance in insurance sales. The increasing media coverage of prominent cyber attacks is also drawing attention to the fact that companies are a worthwhile target for cyber criminals, regardless of their size or the particular sector involved. What are the risks to a company if a cyber attack occurs? The most common scenarios are certainly data theft and data encryption. In 2016, for example, the Neuss Clinic, a hospital in the German city of Neuss, fell victim to a Trojan that encrypted all the data required for the operation of the hospital. The hackers paralysed the city's largest hospital without ever setting foot in it. Everything was brought to a standstill: electronic patient files could not be opened, drug databases were no longer accessible – and to prevent further spread, employees switched off nearly all computers. In short, the entire hospital came to a standstill. The damage, which involved IT security specialists having to clean up every single computer system affected, amounted to around one million euros.

Something similar could happen to a small craft enterprise or a media agency. One wrong click in the attachment of an e-mail and the malware it contains could spread throught the IT network, block access and encrypt data. In such a case, the damage lies not only with the company, but possibly also with the customer, whose data stored on the company server is suddenly no longer secure. In the worst-case scenario, the malware could spread from the infected computer system to third parties, which could give rise to substantial claims for damages. It is just such a scenario that should give independent entrepreneurs food for thought: cyber crime not only endangers business operations and causes considerable financial damage to the company affected – in some cases, it also taps into the data of third parties for which the company is responsible, or it causes damage to further parties. Consequently, in the event of a cyber attack, correct and prompt action to limit and remedy any damage is obligatory.

4 How cyber insurance helps

The greatest added value of cyber policies is that they are more than just insurance to compensate financial losses. Cyber policies provide holistic cover, i.e. they offer preventive services – before and immediately after the occurrence of a loss.

Broadly speaking, the insurance takes effect when the policyholder considers itself exposed to a hacker attack or when data has been stolen. In this case, the costs of restoring data and programs, which can sometimes jeopardise the going concern of a company, are covered by the insurance. Cyber policies provide coverage for both first-party and third-party losses. In addition, the Gothaer coverage concept includes any expenses for necessary hardware replacements or business interruptions, even in the event of a precautionary system shutdown. If the policyholder is a manufacturer, Gothaer also settles claims with regard to manufactured articles affected by the hacker attack.

5 Support in the event of a crisis

Cyber insurance can also assist small enterprises in overcoming a crisis. In the event of a claim, large corporations primarily want to have their losses compensated, whereas SMEs that do not have their own IT department or lack the necessary expertise need more help. A good cyber policy can step in as a manager in the event of a crisis. The support begins with a 24/7/365 hotline allowing customers to obtain around-the-clock assistance in the event of an IT security incident and to report possible attacks.

A cyber attack is above all one thing: time-critical. For this reason, Gothaer always settles all costs incurred for IT security experts brought in during the first 48 hours after the loss was reported – even if it later turns out that there was no hacker attack after all. A prudent cyber insurer should offer its customers crucial assistance services even before something happens. For example, Gothaer assists its customer by performing vulnerability scans and, where required, identifies security gaps before hackers can use them. Staff awareness training is also part of the product. Essentially, insurers use their cyber policies to orchestrate what is currently being discussed as the ecosystem of insurance, and thus as the future of insurance cover.

6 Creating a new (cyber) insurance product

Insurers wanting to offer state-of-the-art products should therefore not only provide their customers with a hotline that is always available, but also offer them their expert knowledge. To reach that point, Gothaer first had to become an expert itself. All insures that have a solid cyber product on the market today agree that getting there has been one of the most exciting challenges of recent years. We had to ask ourselves: what risks are there in the first place and what losses can they cause, and what would be their scale? What can we insure? What do we want to insure? What do we have to insure? And what protective measures should we expect from our customers? Much research was necessary to gain a clear understanding of these issues. For example, the key to correct pricing was loss scenario assumptions for the different customer groups. We used these example losses to estimate costs and determined the insurance benefits required for each individual scenario.

A major challenge in cyber insurance lies in the seemingly unlimited development and diversity of risks, which are also constantly in flux. For example, while there is little change in building insurance, cyber risks resemble a writhing, slippery eel: if you want to catch it, you must throw the largest possible net covering the largest possible area. In cyber insurance, we need to do more than just develop a new product. In order to keep our insurance cover up-to-date during the term of the policy, continuous monitoring and agility in product development are essential: what are the current threat trends, in which direction are technologies and risks developing, and does the insurance product need to be adapted accordingly? On the customer side, a master carpenter or a general practitioner, for example, has little desire to add dealing with the current threats of cyber crime to his or her daily chores. This could provide a great opportunity for insurers: they can take care of the necessary research and assist their customers, taking into account the customer's individual level of protection. After all, policyholders cannot rely only on cyber insurance but must also help to ensure the IT security of their companies.

In addition to the monitoring of threat scenarios, the high complexity of the underwriting processes presented yet another challenge for the development of cyber products. As a typical accumulation risk,[3] cyber damage affects a wide range of insurance lines touching on, for example, third-party liability insurance, business interruption insurance, legal expenses insurance and D&O claims,[4] as well as the engineering lines, electronic equipment insurance and fidelity insurance. Gothaer had to coherently integrate components of all these individual insurance types into one product, mainly related to financial losses. Even in the early stages of product development, it was important to keep an eye on possible later implications, such as other insurance lines that could also be affected by cyber risks.[5]

3 Accumulation risk means the insurer's risk that the occurrence of one and the same fortuitous event simultaneously causes damage to several or many insured units.

4 D&O means Directors and Officers.

5 Regarding the silent cyber issue see also page 73.

7 IT security does not come overnight: obligations to produce evidence

Homeowners wanting to take out home contents insurance should not only have a front door, but also the means to lock it. The same applies to cyber insurance: the prerequisite for taking out insurance is a minimum of security measures to be provided by the policyholder. Among other things, companies are required to install virus protection software on all computers, protect their business data from unauthorised persons by restricting user access and ensure data is regularly backed up. After all, it should not be forgotten that, to put it crudely, the biggest risk factor is in front of the screen: the employee.The best firewall cannot protect users who unsuspectingly click on every e-mail link or use weak passwords. That is why it is up to the companies to raise awareness of cyber risks among their staff. At the same time, users should be encouraged to report suspected hacker attacks immediately instead of remaining silent out of embarrassment and thus risking the spread of damage.

8 The level of protection insurance customers need

As has already been mentioned, insurance customers that are interested in taking out cyber insurance should have a minimum level of security measures, which, incidentally, is not only in the interest of the insurer but also in the policyholder's own vital self-interest. At the same time, the various customers cannot in any way be lumped together. A craftsman, as a commercial customer, requires a different IT environment and thus a different level of protection than a medium-sized manufacturing company. Nevertheless, they both need cyber cover.

Gothaer therefore provides its commercial customers with a catalogue of five technical obligations that they must fulfil. These include, among other things, an anti-virus program and a firewall. In the industrial sector, however, policyholders are required to base their measures for IT security on the generally accepted standards of technology. In addition, there are a large number of standards and norms in daily practice, some of which can be demonstrated to us through the policyholders' risk assessment. These include, for example, the standards of the German Federal Office for Information Security (BSI) as components of the Grundschutz (IT basic protection) methodology or the ISO/IEC standard 27001, which is internationally used and popular in practice.

9 How cyber insurance policies are setting standards

Cyber policies have the potential to set standards. However, this would require that uniform standards for security measures, as currently requested by policyholders, establish themselves within the cyber insurance market. At the same time, the restrictions under competition and antitrust law must always be taken into account. At present, this market resembles more of a patchwork quilt. This is because every insurer expects something different from its customers. While some insurers ask their customers to fill out a questionnaire with only rudimentary requirements, others request information on detailed obligations listed in an extensive catalogue. If the market were to develop uniform basic standards in this regard, which all cyber insurance customers would have to adhere to, this would certainly have a positive impact on society's overall resilience to cyber threats.

The cyber insurance market also shows a mixed picture in terms of the tools used by insurers for their risk analysis and claims settlement. Once again, unification could create standards that lead to more overall IT security.

The other side of the coin is that the standardisation of required security measures and provided services could weaken competition. After all, it is precisely the provision of diverse and heterogeneous processes, services and tools that can give an insurer an advantage over its competitors on this young market and help it win and keep customers. We see that in cyber insurance, much is in a state of flux and that nobody knows what the field of insurers and their product ranges will look like in a few years.

10 Risks and opportunities for cyber insurers

For insurers, cyber policies not only present an opportunity, but also a challenge and a risk. On the positive side, cyber insurance is a rare opportunity for insurers to offer a product in an unsaturated market without being exposed to fierce competition. In addition, above-average premium growth can be expected. A forecast drawn up by a well-known consulting firm in recent years even predicts that over the next 20 years, premium volumes in the double-digit billions could be achieved for the DACH-Region.[6] But even if these forecasted volumes are not reached, cyber insurance is currently the insurance line with the highest forecast growth.

The risky part is that, in contrast to the established insurance lines, there is hardly any reliable data, whether current or past, with regard to cyber insurance. This makes risk assessment, risk modelling and loss estimation technically challenging. Moreover, the empirical values available mostly stem from Anglo-American markets and are transferable to the German market only to a limited extent. A further aggravating factor is that this business line is subject to a very dynamic and extensive risk of change in terms of threat situations and technological developments. Consequently, the expected losses, both in terms of quantity and quality, can be included in the analysis and assessment only with limited certainty. Any assumptions and scenarios made must therefore be continuously monitored so that they can be validated and adapted where necessary.

6 The DACH region includes Germany, Austria and Switzerland.

11 Conclusion: support through the cyber ecosystem

In order to keep the possible effects of cyber damage acceptable for insurers – especially in light of the limited data available and the constantly changing threat situation – all known underwriting options should be applied, in addition to the use of scenarios and parameters, continuous monitoring and the comparison of assumptions. This includes reasonable terms and conditions, careful handling of capacities and the use of sublimitations in the case of extensions of cover that are difficult to calculate.

In addition, some insurers – including Gothaer – are increasingly relying on the support of preventive measures by specialised service providers. The role played by the cyber ecosystem, i.e. the cooperation of insurance undertakings with specialised IT security service providers,

which provides support for risk analysis, loss assessment or risk prevention, is thus increasing in both prominence and importance with regard to the long-term positive development of cyber insurance. Moreover, policyholders, at least many small and medium-sized enterprises, have a need for IT security support and preventive measures, which the cyber ecosystem can provide to a large extent: a win-win situation for everybody.

Imprint

Publisher
Federal Financial Supervisory Authority
(Bundesanstalt für Finanzdienstleistungsaufsicht – BaFin)
Directorate K: Communications
Graurheindorfer Straße 108 | 53117 Bonn
Marie-Curie-Straße 24 – 28 | 60439 Frankfurt am Main
www.bafin.de

Editing and layout
BaFin, Public Relations and Speeches
Editor:
Annkathrin Frind
Tel.: +49 (0)228 4108-7776
Ursula Mayer-Wanders
Tel.: +49 (0)228 4108-2978
Jens Valentin
Tel.: +49 (0)228 4108-2363

E-Mail: perspektiven@bafin.de

Design
werksfarbe.com | konzept + design
Humboldtstraße 18, 60318 Frankfurt
www.werksfarbe.com

Bonn and Frankfurt am Main | 11 May 2020
ISSN 2625-5952

Access
BaFinPerspectives is published on BaFin's website in German and English. The German edition is published under the title "BaFinPerspektiven". If you sign up to the BaFin-Newsletter, you will be informed by e-mail when a new edition is published. The BaFin-Newsletter can be found at:
www.bafin.de » Newsletter.

Typesetting
Mumbeck - Agentur für Werbung GmbH
Schlieffenstraße 60
42329 Wuppertal

Printed by
Druck- und Verlagshaus Zarbock GmbH & Co. KG
Sontraer Straße 6
60386 Frankfurt am Main

Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin)
Federal Financial Supervisory Authority
Communications (Directorate K)
Graurheindorfer Straße 108, 53117 Bonn
Marie-Curie-Straße 24 – 28, 60439 Frankfurt am Main
www.bafin.de