KfW Research
Focus on Economics

»» Harnessing the potential of digitalisation – with data protection and IT security

No. 117, 8 February 2016

Authors: Dr Michael Schwartz, phone: +49 69 7431-8695
Aurelia Muhle, research@kfw.de

Digitalisation holds potential for the future competitiveness of small and medium-sized enterprises (SMEs). In order for them to harness this potential, they must avert the risk of losses. Most SMEs appear to be aware of this. Between 2013 and 2015, almost all SMEs took at least basic precautions to enhance their IT security and data protection.

The KfW SME Panel also demonstrates the urgency of such measures. Between 2013 and 2015, one in three SMEs experienced specific security incidents – small businesses even slightly more frequently than larger SMEs.

SMEs have come a long way. Still, one in two enterprises see the need to step up their level of security. Many SMEs do not have the time or staff to do this, however. Some of them also underestimate the dangers.

In light of the accelerating pace of digitalisation, averting the risk of losses must be understood as an ongoing task.

SMEs must protect the potential of digitalisation

Modern digital technologies and digital networking are rapidly gaining importance (industry 4.0, social media, online banking, cloud computing, etc.). In an era of accelerating digital business processes, many enterprises are challenged to keep pace in order to remain competitive in the future.

Digitalisation holds potential but poses increasing challenges for enterprises to protect their own resources. The need to secure in-house IT infrastructure and protect existing data is therefore more pressing than ever.

Small and medium-sized enterprises in Germany know this and are responding. An additional survey of the KfW SME Panel 2015 shows that SMEs attach great importance to IT security and data protection in their business practice.[1]

SMEs are investing in digital protection

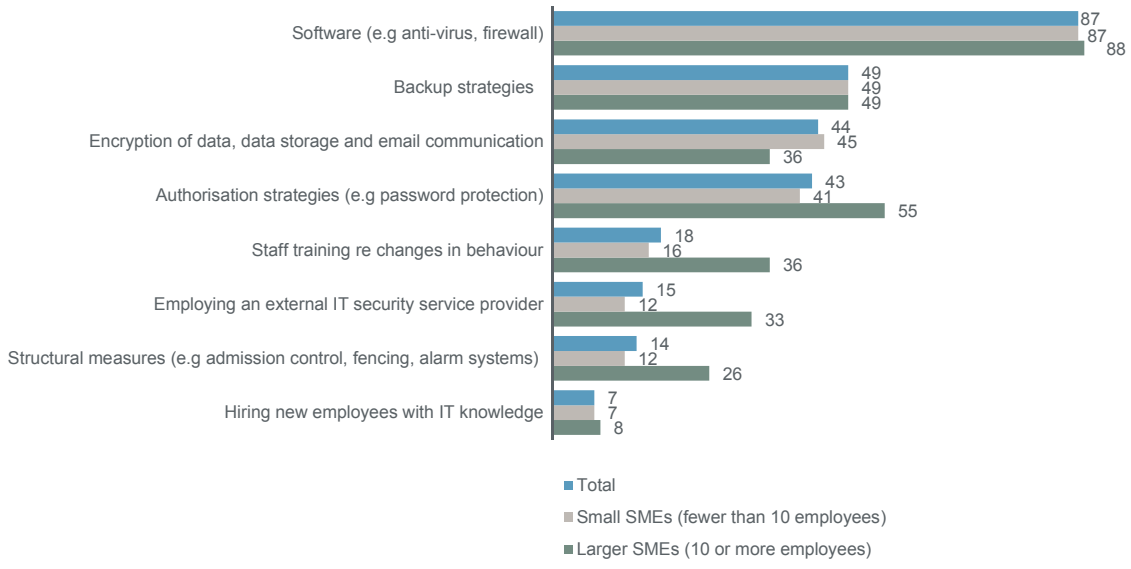
Between 2013 and 2015, 85 % of small and medium-sized enterprises took measures to improve data protection and their IT security. Specific measures were adopted by 95 % of larger SMEs with ten or more employees. This move is influenced by the increasing use of IT applications by bigger enterprises and their often closer integration.

What steps are companies taking?

In the surveyed period, almost nine in ten SMEs implemented corresponding (standard) software strategies (87 %). This step, which is relatively inexpensive and quickly imple-

Figure 1: Measures aimed at improving IT security and data protection (2013–2015)

Proportions of enterprises in per cent, only enterprises that took steps, multiple answers were possible.



Source: KfW SME Panel 2015 (additional survey conducted in September 2015)

mented, is by far the most common measure to achieve greater IT security (e.g. antivirus software, firewalls, spam filters, patch management).

Backup strategies (49 %), use of encryption technology (44 % – e.g. for email communication, USB sticks, hard drives) and implementation of authorisation arrangements (43 % – e.g. passwords, access logging), by comparison, are significantly less common.

More comprehensive and more costly measures such as staff training (e.g. to create awareness of data protection issues and legal provisions), recruiting an external IT security service provider and construction measures are taken considerably more often by larger SMEs with ten or more employees.

Legal requirements complement enterprises' own initiative

SMEs take steps both proactively of their own accord and in response to comprehensive legal requirements (see explanatory box). The higher frequency of staff-related measures taken by larger enterprises may largely be due to the legal requirement for enterprises with ten or more employees to have an internal data protection officer. This data protection officer may be appointed from existing staff or recruited externally. Figure 1 shows both variants.

Are SMEs adequately protected?
More than half say yes ...

More than half the enterprises already regard themselves as well positioned, with 55 per cent of SMEs claiming to be adequately protected. Comparable studies arrive at similar results.[2] This view is common across the entire SME sector and shared by all segments. In the service sector, the proportion is even as high as 58 %.

What this also means is that 45 per cent of SMEs feel they are not yet adequately protected. These enterprises are sceptical with regard to what constitutes an appropriate level of protection. Of concern is also that, at the current margin, expenditure on increased protection measures appears to be stagnating in the SME sector.[3]

Current legislation on data protection in business operations

Enterprises domiciled in Germany are subject to the Federal Data Protection Act (Bundesdatenschutzgesetz - (BDSG)). The provisions of the BDSG cover the protection of data relating to natural persons: Enterprises are obligated to treat all personal data, i.e. individual information about personal or material circumstances of a particular natural person (the data subject), confidentially and securely. They must take steps to protect not only data of customers, employees and business partners but all data that allow conclusions to be drawn on these persons.

Under the BDSG, enterprises are required to take appropriate measures – irrespective of their size or economic sector – to ensure the confidentiality and security of personal data. These include a number of technical and organisational measures that must be reasonably applied and therefore implemented at different levels in the enterprise (e.g. physical admission control, access control, logon control, transfer control).

If at least ten persons (regardless of whether full-time or part-time employees, apprentices etc.) are entrusted with the automated processing of personal data, i.e. in a computing environment, the enterprise is required to have an internal data protection officer. The data protection officer must be able to provide evidence of the required expertise (certificate, degree, professional experience). If an enterprise fails to appoint a data protection officer, its owner or general manager is personally liable and must ensure compliance with the data protection requirements.

In addition to the BDSG, each federal state has its own data protection laws as well as sector and occupation-specific legal provisions. Their application always takes precedence over the BDSG (e.g. confidentiality obligations of doctors and lawyers).

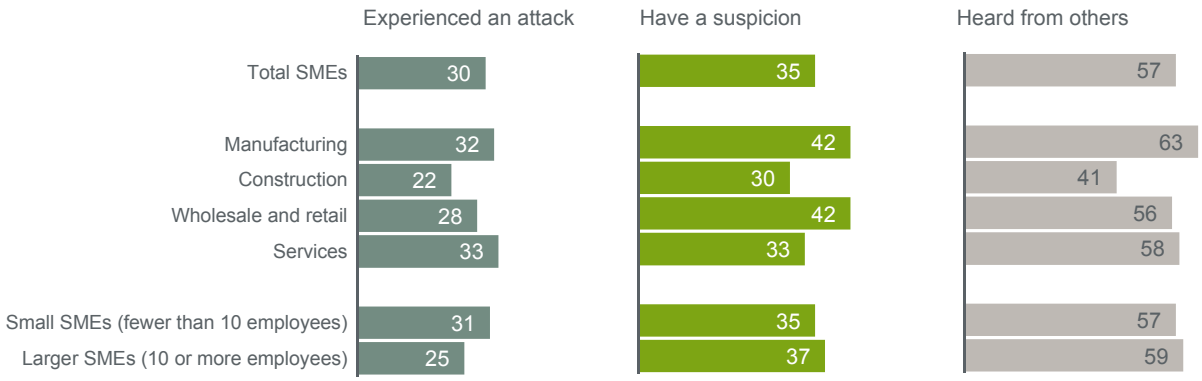
... but security problems are not an exception in the SME sector

The measures adopted by SMEs are necessary. The increasing rate of digitalisation goes hand in hand with broadening target areas. From 2013 to 2015, more than one million small and medium-sized enterprises in Germany were affected by the consequences of an attack on their IT security and data – that is nearly one in three (30 % – Figure 2).

Cybercrime[4] is thus not an exception in the SME sector. Taking into account that the findings 'only' describe a three-year period, it can be assumed that the vast majority of SMEs already have concrete experience.

Figure 2: Frequency of IT security incidents – by sector and size class (2013–2015)

Proportions of enterprises in per cent



Source: KfW SME Panel 2015 (additional survey conducted in September 2015)

Small SMEs are actually targeted more often

The threat to smaller SMEs must not be underestimated. They are subject to a higher number of specific attacks than larger SMEs, with 31 % of them affected compared to 25 %. The public debate is still dominated by (disclosed) cases affecting large corporations such as Apple, Sony, T-Mobile or Microsoft.[5] All of these were recent victims of cybercrime. Public institutions are not being spared either. In the summer of 2015, hackers were able to penetrate the IT network of the German parliament.[6] Nevertheless, the KfW SME Panel has demonstrated that even small businesses are not safe from threats.

It is also obvious that economic sectors are subject to varying levels of threat. Manufacturing firms have to deal with the consequences of attacks on their IT security relatively often or at least have a suspicion. SMEs in the construction industry, on the other hand, are less vulnerable. Across the sector, only 41 % of SMEs reported having heard of incidents from other companies.

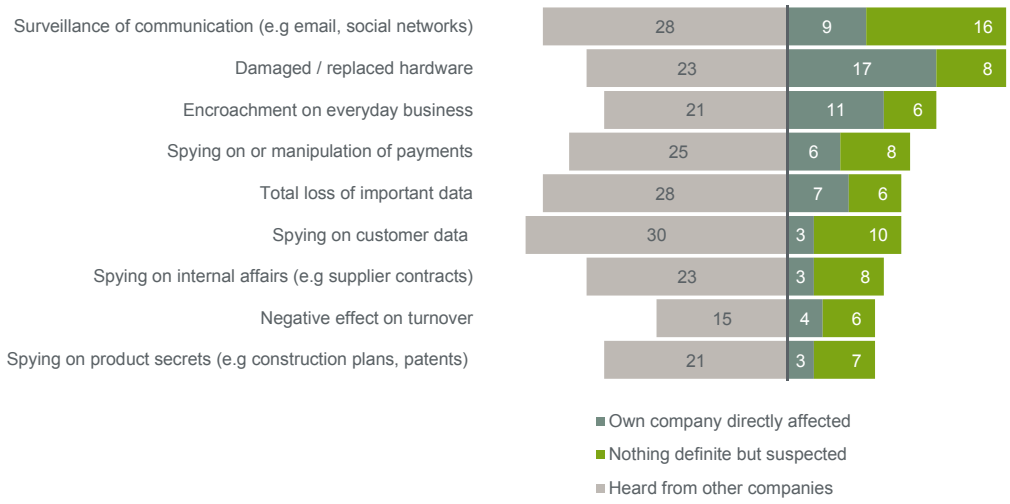
Main focus is on hardware and communication surveillance

Damage to hardware components or necessary replacements are the most frequently reported specific consequences suffered within the enterprise (17 %). Eleven per cent of SMEs reported having been affected in their business operations. The surveillance on corporate communication (for example through emails) affected 9 % of SMEs during the survey period, while a further 16 % at least had a suspicion. Total loss of important data was reported by 7 % of SMEs.

It is important to note that, in the eyes of the public, attacks by external perpetrators are often a primary concern – not least as a result of the highly publicised debate of prominent cases. However, existing findings indicate that the vast majority of damage tends to be caused by an enterprise's current or former in-house staff – either through inadvertent misconduct (such as loss of data carriers, unintentional introduction of harmful software into the company's network) or, much less frequently, intentionally (such as the sale of customers' data).[7]

Figure 3: Specific IT security incidents (2013–2015)

Proportions of enterprises in per cent



Source: KfW SME Panel 2015 (additional survey conducted in September 2015)

High estimate of unreported cases likely

Affected enterprises do not always have have solid evidence of security incidents. Across all cases of damage reported, 35 % of SMEs have a suspicion but no concrete evidence (Figure 2). In other cases attacks remain undetected by the enterprise. How often they occur can only be speculated upon. The number of unreported cases of actual attacks can therefore be higher.

The following finding provides at least an indication: enterprises mentioned having heard of cases occurring in other enterprises more often than they disclosed having experienced an attack themselves (Figure 2).

This is consistent with the fact that, according to the Federal Criminal Police Office, affected enterprises are very reluctant to report incidents:[8] Around 87 % of enterprises that experienced cyberattacks do not report them. There could be many reasons for this, including:

- No report because attack was committed by own staff and is managed in line with in-house policy.
- Attacks are being averted. No damage is detected.
- Attacks on the company remain undetected or are not perceived as such.
- Lack of awareness among the responsible persons.
- Concern over loss of reputation and competitive disadvantages.

What stops enterprises: just costs, no measurable benefit

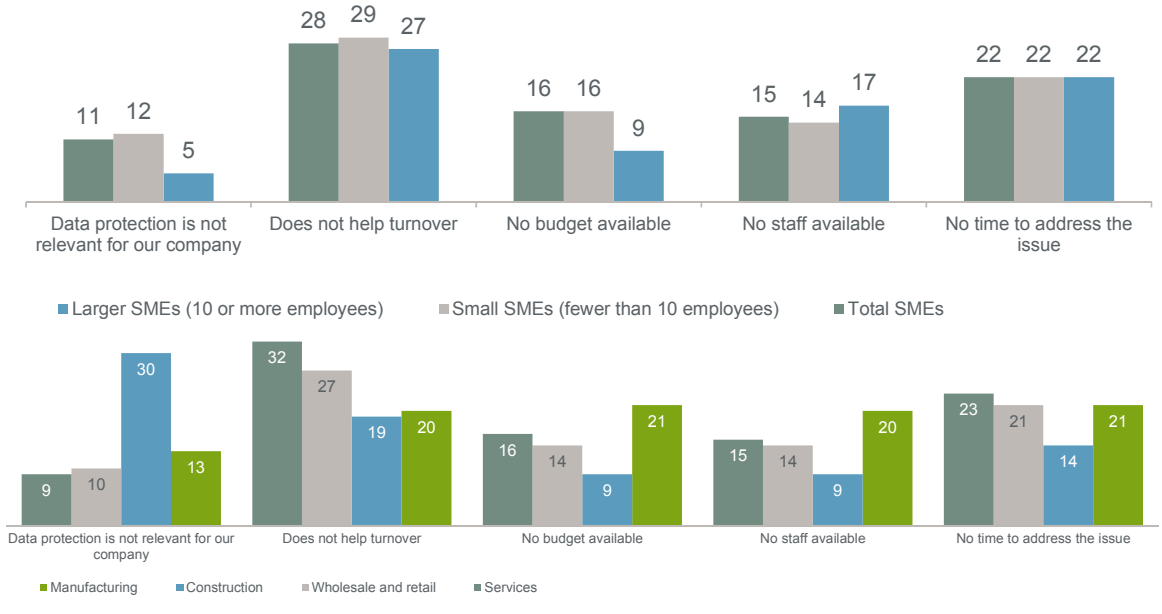
Data protection incurs expenditure and effort, but does not result in a commensurate increase to the company's income. Its immediate contribution to turnover is not discernible – a view shared by many SMEs. That prevents almost two thirds of SMEs (28 %) from making further improvements to data protection. SMEs in service sectors in particular see this as a hurdle.

This view is understandable but poses the danger of misjudging the urgent need for action. Data protection is often not perceived as a pressing problem. The dilemma is that if an attack is ultimately perpetrated against an enterprise's IT security, it can in fact affect turnover – in a negative way. After all, one out of every ten SMEs already suspect having faced fallout in the form of reduced turnover from a cyberattack between 2013 and 2015 (Figure 3). In other words, 150,000 SMEs were specifically affected in these three years alone – a further 220,000 had a suspicion. Awareness of the danger needs to be further sharpened.

An insufficient budget for (further) security measures plays a role for 16 % of enterprises. Larger SMEs have more resources, so in this segment budget constraints are an obstacle for only 9 %. Manufacturers regard budget restrictions as a problem significantly more often (21 %). This can be attributed to the fact that some production plants and machinery require more sophisticated – and hence more expensive – measures to meet the Federal Data Protection Act requirements (see box), such as window locking devices, fencing, alarm systems or security glazing. Necessary investments then compete with other investment measures.

Figure 4: Reasons stated for not stepping up data protection by company size class and sector

Proportions of enterprises in per cent, multiple answers were possible



Source: KfW SME Panel 2015 (additional survey conducted in September 2015)

Enterprises have too little time

Not having enough staff appears to be less of a reason (15 %). However, one in five enterprises (22 %) do not find the time to address data protection systematically. As a consequence, they may end up missing new legal regulations or changes in threat situations.

Thus, German enterprises may not be aware that they are currently barred from transmitting personal data to the USA without specific agreements after the European Court of Justice declared the US Safe Harbor agreement to be invalid in October 2015 (see box).

Not least, it remains to be seen how the European Union General Data Protection Regulation (GDPR) adopted in late 2015 will change business practices in concrete terms. The regulation will replace the EU data protection regulation that has been in force since 1995 and aims to harmonise legal standards on data protection in Europe. The GDPR will largely supersede the current Federal Data Protection Act when it comes into force on 1 January 2018. SMEs should therefore make use of the transitional period to familiarise themselves with the new provisions. For example, it has not yet been finally determined to what extent the new regulation also requires SMEs to have a company data protection officer. Penalties for non-compliance with the provisions then in force will also be much stiffer.

Construction industry is least concerned

Another group of enterprises regards data protection and IT security as not relevant (11 %). SMEs in the construction sector are most prominent, with one in three SMEs seeing no relevance for their own enterprise (30 %). At the same time, however, these SMEs also had the lowest incidence of attacks between 2013 and 2015.

European Court of Justice declares Safe Harbor invalid

European enterprises that wanted to transmit personal data to the USA used to be able to refer to the Safe Harbor agreement. Under that scheme US companies agreed to comply with EU data protection requirements. On 6 October 2015 the European Court of Justice declared the agreement invalid on the grounds that it failed to adequately protect European citizens' data.

Enterprises must now assess whether they will transfer data to the USA (e.g. under a cloud computing arrangement). They will have to act separately on the basis of contractual arrangements with their US business partners when data are to be transferred. Moreover, companies need to have binding internal rules on data transmission that comply with EU standards. The EU Commission has submitted guidelines for this.

Conclusion

Digitalisation holds potential for enterprises' future competitiveness. In order for them to harness this potential they must avert the risk of losses. Precautions in the areas of IT security and data protection are advisable and indispensable. Our findings clearly show this.

More than half of Germany's SMEs feel they are currently adequately protected. Nevertheless, action is still required, especially at staff level, where companies still need to do (much) more than in other areas. Failure to act may prove to be costly in the future. The digitalisation of business processes will continue to increase rapidly – with the addition of new technologies. Protection that may currently be sufficient can quickly become obsolete. Furthermore, various sources have recently observed an increase in electronic crime.[9] So it is all the more important for enterprises to constantly reassess their protective measures.

However, this requires not just one-time adjustments, but permanent efforts: monitoring legal requirements and implementation of new legislation, adopting new standards or simply detecting and closing security gaps in user software. What is crucial here is the need for subject matter expertise at staff level. But this is precisely where companies have been found to be lagging behind, especially small businesses.

IT security and data protection must not be perceived as a 'bothersome' task but, increasingly, as a safeguard for the enterprise's own competitiveness. ■

The database: the KfW SME Panel

The KfW SME Panel (KfW-Mittelstandspanel) has been conducted since 2003 as a recurring postal survey of small and medium-sized enterprises in Germany. The parent population of the KfW SME Panel includes all private-sector companies from all industries with annual turnovers of up to EUR 500 million.

With a database of up to 15,000 companies per year, the KfW SME Panel is the only representative survey of the German SME sector and thus the most important source of data on issues relevant to the SME sector. The main survey of the 13th wave was conducted in the period from 23 February 2015 to 26 June 2015.

The findings presented here are based on a supplementary survey to the KfW SME Panel 2015. This survey was conducted in the period from 8 to 18 September 2015. All enterprises that had already participated in this year's main survey and had provided a valid email address were surveyed. Responses from a total of 2,200 enterprises were evaluated. Owing to their connection to the KfW SME Panel, the special evaluations presented here on the thematic area of data protection and IT security in the small and medium-sized enterprise sector provide a representative picture as well.

Further information and the current annual report can be obtained at www.kfw-mittelstandspanel.de.

[1] See KfW SME Panel 2015, https://www.kfw.de/KfW-Konzern/KfW-Research/KfW-Mittelstandspanel.html

[2] Cf. WIK-Consult GmbH (2012), IT-Sicherheitsniveau in kleinen und mittleren Unternehmen, Studie im Auftrag des Bundesministeriums für Wirtschaft und Technologie (*IT security level in small and medium-sized enterprises, study commissioned by the Federal Ministry of Economics and Technology*), p. 34 (in German).

[3] Deutschland sicher im Netz (DsiN) (2015), DsiN-Sicherheitsmonitor 2015 (*Germany securely on the web (2015), DsiN security monitor 2015*), Berlin (in German).

[4] According to the "Bundeslagebild Cybercrime" (Federal Situation Survey of Cybercrime) of the German Federal Criminal Police Office of 2014, cybercrime refers to all offences targeting the Internet, data networks, information technology systems or their data or perpetrated using this information technology. This covers the following offences: computer fraud (PKS 517500), fraudulent use of access rights to communication services (PKS 517900), falsification of evidentiary data, deception in legal transactions using data processing (PKS 543000), data modification / computer sabotage (PKS 674200), as well as spying on data and interception of data including preparatory acts (PKS 67800).

[5] See inter alia: ZEIT Online (2015), Hacker schmuggeln Malware in den App Store (*Hackers smuggle malware into the App Store*), http://www.zeit.de/digital/datenschutz/2015-09/apple-app-store-malware-xcodeghost. – DIE WELT (2014), Hacker knipsen Playstation- und Xbox-Netzwerke aus (*Hackers switch of PlayStation and Xbox networks*), http://www.welt.de/wirtschaft/webwelt/article135743908/Hacker-knipsen-Playstation-und-Xbox-Netzwerke-aus.html. – Spiegel Online (2015), Hacker erbeuten Daten von Millionen T-Mobile-Kunden (*Hackers snatch data of millions of T-Mobile customers)*, http://www.spiegel.de/netzwelt/web/hacker-erbeuten-daten-von-millionen-t-mobile-us-kunden-a-1055828.html (all articles in German).

[6] See inter alia: Spiegel ONLINE (2015), Cyberattacke auf Bundestag-Es droht ein Millionenschaden (*Cyber attack on German Parliament – damage may be in the millions*), http://www.spiegel.de/netzwelt/web/cyberattacke-auf-bundestag-es-droht-ein-millionenschaden-a-1038178.html. – Süddeutsche Zeitung (2015): Bundestag bekommt Hackerangriff nicht unter Kontrolle (*Parliament fails to bring hacker attack under control*), http://www.sueddeutsche.de/politik/berlin-bundestag-bekommt-hackerangriff-nicht-unter-kontrolle-1.2515345. – FAZ (2015), Hackerangriff auf Bundestag-Anfällige Systeme (*Hacker attack on Parliament – vulnerable systems*),http://www.faz.net/aktuell/politik/inland/hackerangriff-auf-bundestag-anfaellige-systeme-13642190.html# (titles our translation, all articles in German).

[7] Cf. Bundesamt für Sicherheit in der Informationstechnik (Federal Office for Information Security) (2015): Cyber-Sicherheits-Umfrage (Cybersecurity survey) 2015; p. 16 (in German).

[8] Cf. KPMG (2015), e-crime. Computerkriminalität in der deutschen Wirtschaft, Berlin, - Bundeskriminalamt (2013), Handlungsempfehlungen für die Wirtschaft in Fällen von Cybercrime (*Computer crime in the German Economy - Federal Criminal Police Office (2013), recommendations for action by businesses in cases of cybercrime*), http://www.bka.de/nn_238144/SharedDocs/Downloads/DE/ThemenABisZ/InternetKriminalitaet/handlungsempfehlungenWirtschaft.html (in German). – Lower Saxony Criminal Police Office (2013), Survey on security and crime in Lower Saxony.

[9] A number of studies are currently attempting to capture and quantify the threat and damage potential of electronic crime for enterprises. Most of them, however, only take small samples or surveys without claiming to be representative. Nevertheless, the results are clear: electronic crime is on the rise. See for example WIK-Consult GmbH (2012), IT-Sicherheitsniveau in kleinen und mittleren Unternehmen, Studie im Auftrag des Bundesministeriums für Wirtschaft und Technologie (*IT security level in small and medium-sized enterprises, study commissioned by the Federal Ministry of Economics and Technology*) (in German). – KPMG (2015), e-crime. Computer crime in German business, Berlin. – Deutschland sicher im Netz (DsiN) (2015), DsiN-Sicherheitsmonitor 2015 (*Germany securely on the web (2015), DsiN security monitor 2015*), Berlin (in German). – Allianz für Cyber-Sicherheit (*Alliance for Cyber Security*) (2015), Cyber-Sicherheits-Umfrage (Cybersecurity survey) 2015, commissioned by the Federal Office for Information Security, in German.