TECH LAW BRIEFING

Liability Risks for Companies due to Cyber Attacks

The number of companies that are relying on new technological achievements based on Big Data, Industry 4.0 or the Internet of Things is increasing continuously. Companies which digitalise their business processes are very often not only more competitive on the market nowadays but also more vulnerable for cyber attacks. Those attacks are not a random phenomenon anymore: already two thirds of industrial companies in Germany have been a victim of data theft, corporate espionage or sabotage within a two years period.[1] The prior targets have been the company's IT system and communication infrastructure. In one case, the attackers used the spear-phishing method[2] to gain access to the office network of a German steel mill company.[3] Through this, they entered the production network and manipulated the blast furnace, so the employees were not able to shut it down before the company's facilities got damaged.[4]

POTENTIAL DAMAGES CAUSED BY A CYBER ATTACK

Those cyber attacks can cause various damages and might even threaten the company's existence. The above described steel mill case has shown that sometimes damaged facilities need to be repaired or even replaced due to manipulations. In other cases, where sensitive information got decrypted by ransomware, the company might be forced to pay the ransom demand to continue its business. And often the financial cost of the accompanying efforts is even more substantial once a cyber attack has been detected. Usually it will be necessary to hire external IT experts to figure out the scope of the infected computer systems and to remove any virus completely. Furthermore, external servers must be rented for redirecting the current IT systems to a save environment so that pending orders can be processed and the revenue loss minimised. In addition to this, marketing campaigns might be necessary to limit reputation damages and regain the trust of the customers. Beyond that, a company might also face administrative fines when it does or did not comply with legal requirements.

LEGAL FRAMEWORK

When a company has been the target of a cyber attack, different legal obligations need to be taken into account, depending on the consequences of the attack. If the attack has involved a breach of personal data, e.g. the data has been stolen, the company is obliged to notify the competent authority in general about such incident and, if the breach likely results in a higher risk for the data subject, also inform the affected data subject.[5] The violation of these notification obligations can be fined with up to EUR 10 million or 2 percent of the company's annual turnover, which may be imposed by the authority in addition to a potential fine resulting from an actual previous data breach.[6]

Companies acting commercially as website operator or others that are considered service providers under the Federal Telemedia Act,[7] telecommunication companies and critical infrastructure operators[8] have to respect the requirements of the German IT Security Act ("IT-SiG").[9] Critical infrastructure operators are obliged to provide an adequate state-of-the-art security for their IT, and their IT security systems must be checked at least every two years by employees of the company that possess a special qualification acknowledged by the Federal Office for Information Security ("BSI") or external certified auditors.[10] Whereas the IT-SiG does not define what is meant by "state of the art", the BSI specified that the state of the art should be interpreted according to national or international DIN or ISO standards. Violating the requirements of the IT-SiG can be fined with up to EUR 100,000.[11] The field of cybersecurity is also regulated by the EU-directive on security of network and information systems ("NIS-Directive") which has been adopted in 2016 by the EU-Parliament.[12] The transposition of the NIS-Directive into national law has created additional obligations for providers of cloud services, digital marketplaces and online search engines, *inter alia*, duties regarding IT risk management and notifications of cyber attacks.[13] Furthermore, a draft bill for amending the IT-SiG is currently prepared which focuses on expanding the sector's infrastructure considered critical and requires providers to only obtain core components of their critical infrastructure from producers who provide a declaration of trustworthiness which can be reviewed by the BSI.[14]

[1] According to a representative study made by Bitkom available under: https://www.bitkom.org/Presse/Presseinformation/Digitale-Angriffe-auf-jedes-zweite-Unternehmen.html.

[2] A social engineering technique where the attacker approaches an employee of the targeted company via e-mail. The attacker disguises himself as an individual within the recipient´s company, often as superior, and asks for login details or attaches an infected document. When the employee opens the attachment, the attacker can gain access to the company´s network.

[3] The exact circumstances of how the attackers used spear-phishing in this case are not publicly known.

[4] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2014.html.

[5] Art. 33, 34 GDPR.

[6] Art. 83 (4) a GDPR.

[7] Since the IT-SiG is not applicable to non-commercial operators and private persons, they do not have to comply with its requirements.

[8] Whether an operator has to be categorised as critical infrastructure has been specified by the "BSI-KRITIS"-regulation for the energy, water, food, IT and telecommunications, health and transport sectors.

[9] For the text of the IT-SiG see http://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl115s1324.pdf.

[10] Sec. 8a (3) Act of the Federal Office of Information Security ("BSIG"), see also the BSI's "orientation guide".

[11] Sec. 14 (2) BSIG.

[12] Directive (EU) 2016/1148

[13] Sec. 8c BSIG.

[14] So-called IT-SiG 2.0.

BEITEN BURKHARDT

It should be in the interest of board members and CEOs that their company has safeguards against cyber attacks in place. Board members of a German Stock Corporation are personally liable, if they do not monitor developments that might cause damages to the company in the future and implement safety measures accordingly.[15] Even CEOs of a private limited company must exercise the "due care of a prudent businessman".[16] If board members or CEOs do not implement appropriate preventive safeguards and the company, thus, incurs financial losses, they might be faced with compensation claims in the amount of millions of euros.[17]

EXEMPLARY MEASURES TO MINIMISE THE LIABILITY RISK IN CASE OF CYBER ATTACKS

First of all, efficient protection measures against cyber attacks require the sensitisation of management and employees for cybersecurity issues. Seminars and guidelines can help to identify social engineering methods and other techniques attackers use with pleasure to gain access to the company's network for causing further damage. The BSI published IT security guidelines that provide an overview of organisational, infrastructural and technical IT security safeguards.[18] Those guidelines must be implemented and renewed regularly since cybersecurity standards develop continuously. The appointment of a data protection and a compliance officer will help to comply with current and future legal requirements to avoid unnecessary fines. Even though, if all safety guards are in place, a cyber attack can still occur and cause damages like those mentioned above. Therefore, obtaining cyber insurance can help to cover a part of the damages caused by a cyber attack, such as loss of revenue due to business interruptions when the IT system is shut down or the costs of hiring external IT and legal experts.

Susanne Klein
Lawyer | LL.M. | Licensed Specialist for Information Technology Law
BEITEN BURKHARDT Rechtsanwaltsgesellschaft mbH
Frankfurt am Main

Peter Tzschentke
Lawyer
BEITEN BURKHARDT Rechtsanwaltsgesellschaft mbH
Frankfurt am Main

[15] Sec. 91 (2), 93 AktG.
[16] Sec. 43 GmbHG.
[17] See Regional Court of Munich I, decision as of 10 December 2013 – 5 HKO 1387/10.
[18] https://www.bsi.bund.de/EN/Publications/BSIStandards/BSIStandards_node.html.

Imprint

This publication is issued by
BEITEN BURKHARDT
Rechtsanwaltsgesellschaft mbH
Ganghoferstrasse 33 | D-80339 Munich
Registered under HR B 155350 at the Regional Court Munich/VAT Reg. No.: DE811218811

For more information see:
https://www.beiten-burkhardt.com/en/imprint

EDITOR IN CHARGE
Dr Andreas Lober | Lawyer | Partner

YOUR CONTACTS

BERLIN
Luetzowplatz 10 | 10785 Berlin
Dr Matthias Schote
Tel.: +49 30 26471-280 | Matthias.Schote@bblaw.com

DUSSELDORF
Cecilienallee 7 | 40474 Dusseldorf
Mathias Zimmer-Goertz
Tel.: +49 211 518989-144 | Mathias.Zimmer-Goertz@bblaw.com

FRANKFURT AM MAIN
Mainzer Landstrasse 36 | 60325 Frankfurt am Main
Dr Andreas Lober
Tel.: +49 69 756095-582 | Andreas.Lober@bblaw.com

MUNICH
Ganghoferstrasse 33 | 80339 Munich
Dr Axel von Walter
Tel.: +49 89 35065-1321 | Axel.Walter@bblaw.com