Cybersecurity compliance management: implementing legal cybersecurity requirements in a strategic manner

Article by Dr. Carlo Piltz, Stefan Hessel and Karin Potel

Cybersecurity as a Risk and an Opportunity

As a result, companies should take preventive action in an effort to check for possible risks and threats and protect their corporate structures. Attacks may come in a wide variety of forms. At the technical level, companies face risks e.g. from malware, identity theft, social engineering and advanced persistent threats, which seek to target and obtain specific information. But deficient IT security also poses legal risks, given the increasing amount of regulation. With narrower rules for the implementation of IT security requirements, even slight deviations may result in severe fines or contractual penalties, even outside the scope of data protection law. Moreover, if an IT security incident actually occurs, companies will typically face warranty and damage claims from customers and data subjects.

Accordingly, companies operating on the market which plan to successfully digitize must ensure not only that the technical requirements are implemented, but that the legal requirements are satisfied as well. But doing so is much harder than one may think, since there is no uniform statute at either the national or European level which defines the general security requirements for companies in a binding manner. Rather, the legal framework is comprised of many different individual regulations, some of which apply to companies in general and some of which apply only for specific industries or products.

The use of digital technologies is a critical success factor for companies and a requirement for survival on the market in nearly every sector. As a result, products are becoming increasingly digitized and interconnected (e.g. in connection with the IoT), and this is true of production equipment as well (e.g. Industry 4.0 and Smart Factory). The use and exchange of data are no longer limited to individual companies, and are increasingly taking place over the entire supply chain. As processes become more interconnected, operators are becoming more dependent on one another: an IT security incident for a single supplier could affect the entire supply chain, and may even affect the safety of a product on the market.

Cybersecurity Compliance Management Reduces Legal Risks

As a result, companies need a cybersecurity compliance management system, both for the company as a whole and for specific products, which identifies the legal requirements and obligations applicable to the company and helps with their subsequent implementation. For example, the requirements considered by the cybersecurity compliance management system may include rules for the protection of business secrets and know-how from industrial espionage. Here as well, digitization is playing an increasingly significant role, e.g. in connection with the use and protection of machine-generated data. Aspects of IT security law are also coming to the fore right now, as have data protection risks since the introduction of the General Data Protection Regulation (GDPR). In accordance with Article 24(1) in conjunction with Article 32(1) of the GDPR, companies are required to provide adequate protection when processing personal data. The GDPR does not define any specific measures, so that the selection of appropriate measures falls within the company's sphere of responsibility. Given the digital transformation of the automotive industry, more extensive regulations are constantly being adopted for manufacturers and suppliers.

IT security requirements may also arise e.g. from tax regulations, such as the Tax Code. Companies also should not lose sight of indirect IT security requirements, such as those arising from product liability claims or the law governing warranties for defects, which was heavily amended recently by the Digital Content Directive. Depending on the industry and the product, there may also be specific regulations for economic activities which involve elevated risk. In these cases, lawmakers consider the general regulations to be insufficient and insist upon the satisfaction of stricter minimum standards in areas where the risk is particularly high, subject to closer supervision.

One example is that of the statutory requirements for operators of critical infrastructure which, in accordance with § 8a(1) Sentence 1 of the BSI Act, are required to take "adequate organizational and technical precautions" in cases involving elements with critical functions. Pursuant to § 8a(3) of the BSI Act, they are also subject to closer supervision by the Federal Office for Information Security (BSI). Germany's IT Security Act 2.0, which is currently going through the legislative process, will include a whole series of relevant and extensive changes relating to critical infrastructure.

Another example, this time in the field of health care, are digital health applications and prescription health apps, for which special regulations have been adopted with the entry into effect of the Digital Care Act on 19 December 2019. Digital health applications require approval from the Federal Institute for Drugs and Medical Devices (BfArM) for which, in accordance with § 139e(2) Sentence 2 of Book V of the Social Code, applicants

are required to furnish documentation that the digital health application ensures "data security consistent with the state of the art." In order to further specify the requirements, the Federal Ministry of Health has adopted the Digital Health Applications Ordinance pursuant to § 139e(9) of Book V of the Social Code. This Ordinance tightens provisions of the GDPR, e.g. relating to data transfers to third countries, as well as creating extensive IT security requirements via § 4(1) of the Ordinance in conjunction with Annex 1.

Conclusion and First Steps Towards Cybersecurity Compliance

Given the complexity of the current legal situation, and the existence of hidden or indirect IT security requirements in some cases, reducing legal cyber-risks will be a growing challenge for companies. Companies should counter this risk by establishing a cybersecurity compliance management system. In doing so, we typically take the following steps together with our clients:

- identifying applicable laws and requirements for each company and product;
- deriving cybersecurity requirements;
- weighing risks;
- developing, adapting and documenting a comprehensive IT security concept;
- considering legal interactions (e.g. reporting duties, as well as protection of secrets);
- taking legal measures to protect the IT security concept (e.g. through non-disclosure agreements as well as IT legal incident response);
- continuous monitoring for new regulations (early identification) and routine supervision of implementation.

[March 2021]

Company contact: Melanie Schaumann I Head of Marketing & Communications I T > +49 30 / 2332895 0 I E > melanie.schaumann@reuschlaw.de