BIANCHISCHWALD

NEWS

CYBERSECURITY AND COVID-19:

The COVID 19 pandemic means major adjustments for companies, which must be made within a very short time. In reaction to the various restrictions, decentralized working methods have been implemented by many companies. This has led to increased dependence on technology. As a result, an attack by cybercriminals could now have even more far-reaching consequences. From a legal perspective, this requires an appropriate response.

This situation is made more challenging by the fact that in most cases the choice of the infrastructure (hardware, software) was not made after the usual thorough examination and it was not feasible to adequately prepare and train all employees on short notice.

What is cybersecurity?
Cybersecurity means the protection of IT systems, each consisting of hardware, software and the data contained therein. These IT systems are exposed to a variety of threats. The classic example is a cybercriminal who gains unauthorized access to a system in order to either learn secret information or to obstruct, or even destroy, the victim's IT infrastructure. In recent years, attacks involving so-called ransomware have caused major damage and received corresponding media attention. In such attacks, the victim's data is made unreadable by technical means (e.g. encryption). In consideration for reversing this process, the attacker usually requests money or crypto currencies.

From a technical point of view, it should be noted that apparently minor changes to the IT infrastructure can cause substantial risks that are not always detected in time. As an example: If employees connect to their private WiFi instead of the company's internal network, numerous additional points of attack arise that are largely beyond the control of the cybersecurity provider. This is true even if the server is accessed via a secure connection (e.g. via a Virtual Private Network, VPN for short).

Attacks that are known under the term «social engineering» are equally pervasive. What they have in common is that cybercriminals try to influence the victim to cause a certain behaviour. A well-known example is the so-called phishing attack. The attacker poses as a legitimate institution in order to trick the victim into revealing secret information (such as passwords, bank or credit card data) or to trigger payments. With newly introduced decentralized working methods, companies are much more susceptible to such attacks. Suddenly, everyday interactions, which previously took place exclusively in personal exchanges, are now carried out via electronic means of communication. This creates a new vulnerability for companies.

What are the legal aspects of cybersecurity?
In addition to the operational and financial risks and possible damage to reputation, there are also legal obligations regarding cybersecurity. Which specific obligations apply to a concrete case is a key question. Under Swiss law, there is no general obligation to protect the integrity of IT systems. Instead, various laws contain provisions that explicitly or implicitly require the protection of IT systems.

Criminal law
Special attention should be given to those rules whose violation may have criminal consequences. Among the best-known examples are the protection of professional secrecy, trade secrets and banking secrecy. Furthermore, the failure to adequately protect IT systems may constitute an offence of criminal mismanagement, and also the violation of certain data protection provisions is also a criminal offence.

These criminal provisions usually only apply in case of intentional commission of the crime. In most cases, a complaint by an authorised person is further required. For this reason, the risk of conviction is often quite low. Nevertheless, a legal review is advisable in view of the potentially grave consequences.

Civil law and administrative law
There are also numerous provisions in civil and administrative law which require or presuppose the integrity of IT systems. Some of these provisions, which are relevant for the majority of Swiss companies, are highlighted below.

The rules and regulation on data protection, namely the Swiss Federal Data Protection Act and the associated ordinance, are highly relevant. In general, this is an important source of law in connection with the protection of IT systems. It expressly stipulates that personal data must be protected against unauthorised processing by appropriate technical measures. Due to the broad definition of the term «personal data», this obligation applies almost without exception to all Swiss companies, regardless of their legal form.

The Swiss Federal Ordinance on Accounting Ledgers also contains principles that must be observed when documents are stored electronically. Regarding cybersecurity, the primary obligation is to ensure the integrity (authenticity and unfalsifiability) and availability of the documents. This must be observed by all companies that are subject to the obligation to keep accounts according to the Swiss Code of Obligations. In this context, further storage obligations, for instance in tax and social security legislation, have to be taken into consideration.

There are also various industry and best practice standards. These include regulations for financial institutions and ISO certification which specify data protection and other relevant standards. In addition, there may also be requirements from non-governmental organisations that impose further obligations in the form of self-regulation (e.g. confidentiality obligations).

In addition, contracts often contain an obligation to protect IT systems as well. This is obvious in cases where there are clauses prescribing confidentiality, both as secondary obligations or even as the main obligation (so-called Non-Disclosure Agreement or Confidentiality Agreement). Furthermore, other obligations assumed in contracts may also (indirectly) require the protection of IT systems. For example, there may be an obligation to account for the activities performed under the contract. This is only possible if the electronic documents required for this are appropriately secured.

The principal risk associated with the violation of these provisions is the potential liability for damages. The amount is determined according to the damage caused by the violation of the provision. For contractual obligations, there is also the risk of a contractual penalty.

The failure to secure IT systems can constitute a breach of duty on the part of the supervisory bodies of a legal entity (the administrative board of the company limited by shares [«Aktiengesellschaft»] as well as the management of the GmbH). The members of the supervisory body are subject to a strict duty of care and must safeguard the interests of the company in good faith. In the case of delegation of the operative management, the delegees must be duly supervised. Any such breach of duty may cause the liability of the bodies' individual members, including with their personal assets.

Further legal issues
The decentralised working methods and the increased use of technology outlined above entail a number of other relevant legal questions, which go beyond the core issue of cybersecurity:

- May the private electronic devices of employees (laptop, mobile phone) be used for business purposes? Under what conditions? Is there a right to compensation?
- Is it permissible to store documents in the cloud? What must be taken into account? Does a paper copy have to be kept in any case?
- Can a document be legally signed without a handwritten signature

Many suppliers of goods and services are currently considering offering their products and services through new distribution channels. One widespread option is distribution via the Internet. When implementing an online shop in Switzerland, various legal requirements must be observed (see in detail the BianchiSchwald Newsletter on e-commerce).

What needs to be done?
The development of IT systems – as well as the corresponding threats – regularly undergo fundamental changes. As a result, the protection of IT systems requires continuous monitoring and adaption. Only if the legal obligations regarding cybersecurity are sufficiently known, will the company be able to define appropriate measures. The legal analysis of the initial situation is therefore an important component of any cyber security strategy which should be reviewed periodically to ensure that it is up-to-date.

The decentralized working methods implemented in response to the COVID-19-related restrictions lead to additional need for review of the cybersecurity strategy. The potential impact on cyberse-

curity needs to be evaluated based on the concrete measures taken by a company. The following questions can indicate whether a review is in order:

- Has a new IT system been introduced in the company which affects a central process or which for other reasons performs an important function for the company?
- Were the employees adequately introduced to the new IT system?
- Are all employees aware and informed about the additional risks to the security of IT systems?
- Is it planned to test the effectiveness of the protection of IT systems?

It is particularly worthwhile, especially when adapting the business model in response to a crisis (such as the COVID-19 pandemic), to identify any legal challenges at an early stage and develop solutions.

If you have any questions, please feel free to approach your contact person at BianchiSchwald.

CHRISTOPH GASSER
Attorney-at-Law, Dr. iur., LL.M. University of Michigan
Non-permanent Judge at the Swiss Federal Patent Court
Partner

ADRIAN TRUTMANN
Attorney-at-Law, MLaw
Associate

THIERRY BURNENS
Attorney-at-Law, M.A. HSG
CIPP/E
Associate

BIANCHISCHWALD GMBH
mail@bianchischwald.ch
bianchischwald.ch

GENEVA
5, rue Jacques-Balmat
P.O. Box 5839
CH-1211 Geneva 11
P +41 58 220 36 00
F +41 58 220 36 01

ZURICH
St. Annagasse 9
P.O. Box 1162
CH-8021 Zurich
P +41 58 220 37 00
F +41 58 220 37 01

LAUSANNE
12, avenue des Toises
P.O. Box 5410
CH-1002 Lausanne
P +41 58 220 36 70
F +41 58 220 36 71

BERNE
Elfenstrasse 19
P.O. Box 133
CH-3000 Berne 15
P +41 58 220 37 70
F +41 58 220 37 71