N

Monthly
Newsletter
March 2023

IT Security and Cybercrime

Schellenberg Wittmer

Cybersecurity – Ten Legal Commandments for Prevention

Roland Mathys

Key Take-aways

1.
In the context of cyber prevention, legal aspects must be considered in addition to technical and organizational ones. This is not done sufficiently today.

2.
The most important legal steps for action can be summarized in ten points and be implemented with reasonable effort.

3.
If preventive legal measures are neglected, a company risks various disadvantages, ranging from breaches of contract to sanctions.

Introduction

Cybercrime is on everyone's lips. Hardly a day goes by without a major company or public authority falling victim to a cyberattack. Cyberattacks are now perceived as **one of the biggest risks from a business perspective**. With the ever-growing threat of cyberattacks, awareness for the need of preventive measures has also increased greatly, with a focus on technical and organisational steps. **Legal measures** in the field of cyber prevention, however, **are still hardly taken** – wrongly so, because much remains to be done in this area in order to be prepared for the event of a cyber attack. In the following, the most important preventive recommendations from a legal perspective are summarised in terms of ten commandments for action.

Little attention is paid to the contractual dimension of cyber incidents.

1 Information security

Information security is primarily understood as a technical matter, but it also has a legal dimension. According to the EU General Data Protection Regulation (**GDPR**), appropriate technical and organisational measures must be taken **to ensure data security**; otherwise, there is a threat of severe fines in the millions. Also under the upcoming Swiss Data Protection Act (**DPA**), non-compliance with minimum data security requirements will be punishable and may be sanctioned with a fine of up to CHF 250,000.

Inadequate information security can also lead to a violation of **secrets protected by criminal law** (e.g. medical secrecy) and can be punished in the case of (contingent) intent and, for the banking secrecy, even in the case of negligence. Legal obligations to ensure information security can also be found in sector-specific regulations (e.g. financial industry) as well as – specifically directed at corporate bodies – in the Swiss Code of Best Practice for Corporate Governance.

2 Cyber Emergency Response Team

A company should have an emergency response team in place that can act in the event of a cyber incident and take the necessary measures. Such a Cyber Emergency Response Team (CERT) must be **formed and briefed in advance**; once the cyber incident has occurred, there will be no time.

The CERT must be composed of the **appropriate roles and staff members** so that it functions well in the event of a crisis. In addition to the subject matter experts, representatives from information security, communications and legal/compliance should be included in the CERT. The upper management of a company must also be involved in the CERT. Depending on the size and organisation of a company, external service providers should be retained in addition to internal specialists (see below).

The **role of lawyers** in the CERT is to initiate all necessary legal steps in a timely manner and in the right sequence in the event of a cyber incident. This includes contacting the cyber insurance company (see below), reporting data breaches to authorities and affected data subjects, initiating an internal investigation, filing a criminal complaint or preparing the defence against third-party claims.

3 External specialists

External service providers such as security experts, IT forensic experts, "negotiators" for ransom demands and lawyers should be onboarded at an early stage. **Mandate agreements** should be put in place with these service providers and checks made for conflicts of interest. If a company starts the onboarding only after a cyber incident has occurred, valuable time is lost and the company is in an unfavourable negotiating position.

Contact points and lines of communication should be defined for all service providers (including on-call availability as needed). Furthermore, the service providers should be familiarised with the specifics of a company and the relevant processes (see below) in order to respond quickly in an emergency.

4 Processes, guidelines and templates

As part of the preparation for a cyber incident, relevant processes should be documented and guidelines established. This applies in particular to the **process for reporting a data breach**, which must happen within a short time period after becoming aware of such an incident and its scope. Security-relevant guidelines are also crucial, e.g. instructions for employees on how to deal with cyber risks. In addition, templates for internal and external communication should be prepared, which can eventually be quickly adapted to the specific circumstances of the cyber incident if necessary.

Once put in place, the documentation must be **validated and updated on an ongoing basis**, for example if new threat scenarios arise, changes to the IT infrastructure are made or new legal requirements must be complied with. On the one hand, the aforementioned documentation serves to act quickly, systematically and in a targeted manner in the event of a cyber incident and thus to minimise the effects of the incident. On the other hand, the purpose of the documentation is to prove compliance with minimum data security requirements and the implementation of pertaining measures.

5 Compliance

Companies that are **not in the primary focus** of data protection authorities sometimes neglect data protection compliance. However, this can quickly change when a cyber incident occurs and a company suddenly appears in the spotlight of the authorities. If it then turns out that the company has not

implemented data protection requirements in compliance with the law, further trouble may arise.

An example is the case of a company that notified a data breach to the data protection authority in an EU Member State. Triggered by the preparation of such notification, it became apparent that the privacy notice on the company's website also had to be adapted, that an EU representative had to be appointed and that a register of processing activities had to be set up.

Cyber insurance can cover a residual risk, but is not a panacea.

6 Authorities

In addition to retaining external experts in the CERT, contacts should also be established and maintained with the authorities responsible for handling cyber incidents. These include **data protection, criminal and other supervisory authorities** (e.g. in the financial sector).

First of all, the company must determine which authorities are **competent in terms of location and subject matter**. If a company has access to different authorities, the question arises as to which authority has the greatest expertise and experience in dealing with cyber incidents; in the case of criminal authorities, this regularly applies to Swiss authorities in those cantons having set up their own cybercrime units. Within the competent authority, the relevant contact persons should be identified, along with their contact details, in order to ensure the most direct access possible.

It is also advisable to seek an **exchange** with representatives of the authorities in the context of cyber prevention. This allows the authorities to learn more about the company and to assess how critical a cyber attack can be for the company. In some cases, companies (e.g. operators of critical infrastructures) discuss the operating procedures in the event of a cyber incident with the authorities in advance. In our experience, authorities are usually open-minded and cooperative towards such exchanges.

7 Contracts

Cybersecurity has increasingly become the subject of contractual agreements. Contracts with key business partners should be reviewed for **provisions around cyber security** to avoid breaches of contract.

This review should clarify whether a contract prescribes **minimum cyber security** requirements and whether the company complies with them. Furthermore, it should be assessed in advance whether a cyber incident (possibly depending on its severity) constitutes a breach of contract and what legal consequences it entails. It is also important to know whether (and within what period of time) the contractual partner must be **informed** about a cyber incident.

All these findings should be recorded in an **inventory** that is regularly updated and is also available offline (e.g. as hard copy). Ironically, we have come across cyber incidents where access to such documents failed precisely because they were encrypted in the course of a ransomware attack.

8 Supply chain and service providers

Often, a **security vulnerability** does not exist at the attacked company itself, but in its supply chain or at an (IT) service provider (e.g. cloud provider or software supplier). With regard to business-critical third parties, a contractual due diligence must therefore take place in addition to the technical due diligence.

As part of the **contractual due diligence**, the contract with the third party must be analysed in particular with regard to the following topics: Security standards and measures, certifications, audit rights, vulnerability testing, standard of care, contractual representations and warranties, duty to inform (e.g. access to forensic report), duty to assist in cyber incidents and remuneration, remedies (e.g. liability, extraordinary termination), insurance coverage and other collaterals.

If the contract does not contain **sufficient provisions** on these points, a (re-)negotiation is recommended. If this does not lead to an improvement, termination of the contract (or abstaining from the conclusion of the contract) should be conceived.

9 Training and awareness

The human factor is one of the key vulnerabilities for cyber attacks, be it through phishing attacks, virus-infected file attachments or sophisticated social engineering. Accordingly, it is important to raise awareness about cyberattacks, to illustrate typical attack patterns and to train the right behaviour. Such **training** must take place regularly and, in view of technical progress, with up-to-date content.

Training is one of the organisational measures to ensure sufficient information security. Neglecting training measures is therefore to be classified as a breach of data security with corresponding consequences.

10 Insurance

Despite all preventive measures, a **residual risk** always remains; (cyber) insurance may provide coverage at best. Under no circumstances, however, should one rely solely on insurance and neglect the preventive measures described above.

In the first place, the question arises whether and under what conditions cyber incidents are covered by insurance at all. As a matter of rule, insurance companies tend to require proof of a **minimum level of technical resilience**. It is then necessary to check which **types of damage** are covered (e.g. ransom payments, indirect damage due to business interruption, expenses in connection with filing a criminal complaint).

A company should also know in advance which **obligations must be observed in the event of an incident**.
In addition to damage notification, these duties typically inclu-

de documentation obligations, measures to mitigate damage or cooperation with specific external service providers.

Finally, it is advisable to compare and **benchmark** different cyber insurance providers along key performance indicators. Considerable differences exist, for example, in the length of time it takes for cost approval which – in our experience – can range from less than one hour to several days.

Conclusion

In addition to technical action items, legal measures are also of fundamental importance in the context of cyber prevention. Most of these precautions are not rocket science and can be implemented with manageable effort. This makes it all the more important to pay due attention to these aspects.

Roland Mathys
Partner Zurich
roland.mathys@swlegal.ch

Peter Burckhardt
Partner Zurich
peter.burckhardt@swlegal.ch

Louis Burrus
Partner Geneva
louis.burrus@swlegal.ch

Clara Poglia
Partner Geneva
clara.poglia@swlegal.ch

Schellenberg Wittmer Ltd
Attorneys at Law

Zurich
Löwenstrasse 19
P. O. Box 2201
8021 Zurich / Switzerland
T +41 44 215 5252
www.swlegal.ch

Geneva
15bis, rue des Alpes
P. O. Box 2088
1211 Geneva 1 / Switzerland
T +41 22 707 8000
www.swlegal.ch

Singapore
Schellenberg Wittmer Pte Ltd
6 Battery Road, #37-02
Singapore 049909
T +65 6580 2240
www.swlegal.sg