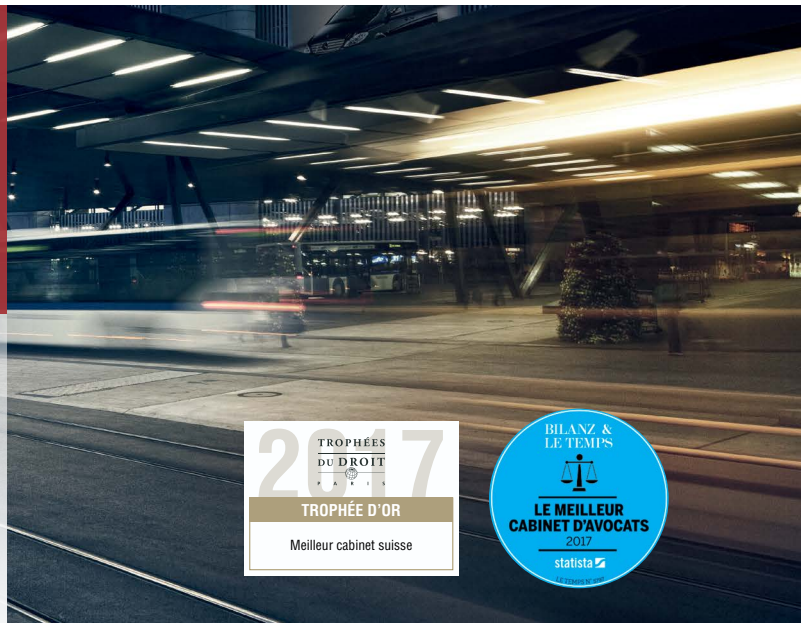
ATTORNEYS AT LAW

SCHELLENBERG WITTMER

FEBRUARY 2018

Newsletter

Author:
Roland Mathys



ICT / DATA PRIVACY

Prevention, action, reaction – legal handling of cyber risks

With the intensified business pervasion by technology, white-collar crime is also increasingly shifting into the digital sphere. Hardly any company has not yet been targeted or even become the victim of a cyber-attack. Although companies are becoming more and more aware of this new form of threat, there is often a lack of clear ideas as to what needs to be done to prevent and cope with it.

1 INTRODUCTION

Cyber-attacks have become increasingly widespread and meaningful in the recent past. Prominent cases such as that of ransomware "Petya", which temporarily paralysed the IT systems of numerous large companies, have sharpened attention for this new form of danger. Cyber-attacks, however, take place on a daily basis. In recent studies, almost 90 percent of the surveyed companies stated that they had been affected by cyber-attacks in the past twelve months.

Cyber-attacks target **almost all companies**, regardless of industry, size or jurisdiction. The global group of financial companies is similarly affected by this as local SMEs. Accordingly, cyber risks and cybercrime are nowadays classified as one of the **greatest threats** to businesses in numerous surveys. This makes it all the more surprising that measures to defend against and manage cyber-attacks are often missing or only exist at the very beginning.

This **enforcement backlog** becomes clearly evident, for example, in the duration elapsing between a successful cyber-attack and its eventual discovery: in about 85 percent of all cases, a successful cyber-attack is only detected after five months; on average, a successful cyber-attack remains hidden even for about 250 days and thus about eight months. During this time, an affected company is particularly vulnerable, and the attackers remain largely undisturbed.

This newsletter aims to show how cyber risks are dealt with from a **legal point of view**. A distinction is made here between the three phases of prevention to ward off attacks, immediate action in the event of a (successful) attack, and reaction in the wake of an attack.

2 PREVENTION

2.1 NECESSITY

Prevention, i.e. the implementation of measures to preclude cyber-attacks from reaching their target, should be at the beginning of any defence strategy against cyber-attacks. Such measures are not only recommended for reasons of self-protection and the reputation of a company, but are also partly prescribed by law and thus form part of **corporate compliance**.

> "In about 85 percent of all cases, a successful cyber-attack is only detected after five months."

A general and comprehensive **obligation to prevent** cyber risks cannot be explicitly derived from the applicable laws in Switzerland. However, this task can be understood as part of the overall management of the company (Art. 716a of the Swiss Code of Obligations) and thus as a **duty of the Board of Directors**. This task is further specified, for example, by the Swiss Code of Best Practice for Corporate Governance issued by *economiesuisse*, the umbrella organisation of the Swiss business associations, according to which the Board of Directors must ensure risk management and an internal control system adapted to the company (Principle 20). Given the current threat situation, prevention of cyber risks is one of the measures to be taken by the Board of Directors.

A concretisation for personal data can be found in the Swiss **Data Protection Act (DPA)**: It provides that personal data must be protected against unauthorised processing by appropriate technical and organisational measures (Art. 7 DPA); what this includes in detail can be derived from the pertaining Ordinance (**ODPA**; see Art. 8 et seq.). The draft of the currently revised DPA places greater emphasis on the risk-based approach to data security (see Art. 7 draft DPA). As an example, the Dispatch expressly mentions protection against malware (BBl 2017 6941 et seq., 7031). The EU General Data Protection Regulation **(GDPR)**, which comes into force on 25 May 2018, also states data security as a key principle (Art. 32 GDPR).

Explicit rules for the prevention of cyber risks also exist for individual economic industries, especially in the **finance sector**. The Circular 2008/21 "Operational Risks - Banks" of the Swiss Financial Market Supervisory Authority **(FINMA)** stipulates since 1 July 2017 that the Executive Board must implement a risk management concept for dealing with cyber risks (Principle 4). This concept should cover at least the following aspects:

- Identification of the specific threat potentials;
- Protection of business processes and technology infrastructure;
- Real-time detection and recording of cyber-attacks;
- Responding to cyber-attacks by timely and targeted measures;
- Ensuring the timely recovery of normal business operations after cyber-attacks through appropriate measures.

According to the Circular, the management's tasks also include regularly reviewing the effectiveness of the concept and measures through vulnerability analyses and penetration tests.

2.2 MEASURES

The arsenal of preventive measures to avert cyber risks is large. First of all, every company should set up a **cyber-security program**. This program defines basic responsibilities, such as the designation of a Chief Information Security Officer (CISO). The involvement of top management is crucial to this. The program also sets security guidelines and monitoring systems for the rapid detection of cyber-attacks; especially in the case of monitoring systems, new solutions have recently conquered the market having led to reliable findings by using the mechanisms of artificial intelligence. The effectiveness of the established processes and systems should be tested regularly, e.g. by means of simulated attacks.

> "There are explicit rules for the prevention of cyber risks for individual economic industries, especially in the finance sector."

Every company must be or become aware of the risks it is exposed to. An inventory of sensitive data and infrastructures is drawn up as part of such a **risk assessment**. Possible threats and potential attacks are identified, whereby the human factor and especially the potential of internal attacks must not be underestimated. A gap analysis is then used to locate gaps and weak points in the current protection and defence system and eliminate them with appropriate technical and/or organizational measures. Insurance coverage must be considered for remaining risks (see below).

The risk assessment should not be carried out by the company in isolation, but with **bearing in mind the role third parties**. Contracts with third-party providers of essential services (e.g. data hosting) must be thoroughly examined to see whether the aspect of data and information security is given sufficient consideration. Providers of business-critical services should be subjected to an actual cyber security due diligence.

Employee training is considered an essential element of preventive measures. On the one hand, this is intended to raise awareness of the potential threat posed by cyber risks; on the other hand, it is intended to provide employees with the most important principles for preventing cyber-attacks and for correct behaviour in the event of a successful cyber-attack, for example by providing mock trainings under realistic conditions.

Finally, the preparatory measures include the setup of a cyber-incident response plan, which describes how to proceed in the event of an emergency (cf. right below).

3 ACTION

Every company must be prepared for the event that a cyber-attack reaches its target despite preventive defence measures. In addition to the **rapid detection** of a successful

attack, the focus is on **correct behaviour in an emergency**. To this end, responsibilities must be clearly defined and the tasks properly assigned.

3.1 TEAM

In the event of an emergency, the company's incident response team must act immediately. This team is made up of representatives from the areas of IT, law/compliance, HR, communications, the business line affected by the attack and top management. The team should also include selected external specialists (e.g. cyber forensic experts or lawyers).

3.2 TASKS

The team's first tasks include **assessing the scale of the cyber-incident and taking immediate action to minimize damage** (e.g. by separating all devices from the network to prevent the spread of malware). Business continuity must then be ensured in an emergency setup and at short notice. In the medium to long term, the return to normal business operations must be planned and initiated.

The incident response team must also check whether and how the incident is **communicated** internally and externally and whether formal notifications are necessary (cf. below). The question also arises to what extent an **internal investigation** of the incident should be initiated and whether further steps (e.g. criminal complaints or disciplinary measures) are required. Finally, the team should consider how similar incidents can be avoided in the future.

"In addition to the rapid detection of a successful cyber-attack, the focus is on correct behaviour in an emergency."

4 REACTION

4.1 NOTIFICATION

After a successful cyber-attack has occurred, it must be clarified promptly whether and to whom the incident must be reported. Such a notification requirement may primarily arise from **data protection law**. The current DPA does not expressly state any obligation to report security-relevant incidents. In contrast, the draft of the revised DPA stipulates that, under certain conditions, the Federal Data Protection and Information Commissioner and, if necessary, the affected individuals must be informed "as soon as possible" about a cyber-incident (Art. 22 draft DPA). The same applies under the EU General Data Protection Regulation (see Art. 33 et seq. GDPR). Additionally, there are **reporting obligations for individual sectors in accordance with specific laws** (e.g. for telecommunications service providers, for financial market supervisees, or in the health sector).

In the case of listed companies, a duty to report a cyber-incident may also arise from the rules on **ad hoc disclosure**. Accordingly, all information that is likely to have a significant impact on the share price of a company must be disclosed. Even where there is no statutory notification requirement, disclosure can be recommended, for example for reasons of reputation, best practice or to minimise potential damage.

4.2 LEGAL FOLLOW-UP

Once a cyber-incident has occurred, the company must consider what legal action should be taken against the perpetrators of the attack. Civil and criminal law measures as well as individual special instruments are available.

Under **civil law**, claims for injunctive relief, removal or damages may be based on breaches of contract (e.g. by customers or suppliers) or on tortious acts; in the latter case, illegality is usually due to the committing of a criminal offence, an infringement of trademark or copyright, a personality or data protection infringement or unfair competition. Under **criminal law**, the spectrum includes on the one hand specific cyber crime offences (e.g. hacking, data theft or damage, computer fraud) and on the other hand "classic" criminal offences (e.g. fraud, blackmailing, coercion, forgery of documents or breach of secrecy), often in combination.

The Ordinance on Internet Domains **(OID)**, which has been revised since 1 November 2017, introduces a new instrument for **blocking domain names of illegal websites**. The remedy applies to websites of the top-level domains .ch and .swiss through which phishing is practiced or malware is distributed or which support such illegal activities.

There is also the possibility to report cyber-incidents of any kind to the Reporting and Analysis Centre for Information Assurance MELANI (www.melani.admin.ch) or to the Cybercrime Coordination Unit Switzerland CYCO (www.kobik.ch). However, due to the large number of reports and limited resources, these institutions will often not be able to investigate reported incidents in detail.

As outlined above, a large arsenal of legal measures is generally available; however, the inherent circumstances and specific challenges of cybercrime, in particular the anonymity and virtuality of the perpetrators, the international dimension and the time factor, often make the enforcement of these measures appear to be less promising.

4.3 INSURANCE

Even with comprehensive preventive measures, the occurrence of a cyber-incident cannot be completely ruled out, which raises the question of the insurability of cyber risks. **The market for cyber insurance** is still relatively young in Switzerland, but is growing. The insurance models available to date cover third party losses (e.g. liability claims) and/or "own losses" of the affected company (e.g. costs for crisis management, costs for data recovery or the consequences of a business interruption).

In the case of cyber insurance, it is advisable to **examine** in detail which risks are covered, which due diligence obligations on the part of the policyholder are assumed (especially preventive technical and organizational measures) and which obligations the policyholder has in the event of damage (e.g. reporting or notification obligations).

5 OUTLOOK AND CONCLUSION

In Switzerland, numerous **political advances** in the field of cybercrime can currently be observed. These range from the creation of specific competence centres and centralized contact and coordination points to the introduction of new reporting requirements (e.g. for operators of critical

infrastructures). The need for action has thus also been recognized by legislators and authorities.

Companies in Switzerland are becoming increasingly aware of cyber risks. However, the **implementation of appropriate measures is often still lacking**. The proactive management of cyber risks is becoming an increasingly central pillar of corporate governance and compliance.

Contacts

The content of this Newsletter does not constitute legal or tax advice and may not be relied upon as such. Should you seek advice with regard to your specific circumstances, please contact your Schellenberg Wittmer liaison or any of the following persons:

In Zurich:

Roland Mathys
Partner
roland.mathys@swlegal.ch

Peter Burckhardt
Partner
peter.burckhardt@swlegal.ch

In Geneva:

Benjamin Borsodi
Partner
benjamin.borsodi@swlegal.ch

Louis Burrus
Partner
louis.burrus@swlegal.ch

CHAMBERS EUROPE AWARDS 2014 WINNER SCHELLENBERG WITTMER Switzerland Law Firm of the Year

WWL AWARDS Switzerland FIRM OF THE YEAR 2015

WWL AWARDS Switzerland FIRM OF THE YEAR 2016

SCHELLENBERG WITTMER LTD / Attorneys at Law

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

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

SINGAPORE / Schellenberg Wittmer Pte Ltd / 6 Battery Road, #37-02 / Singapore 049909 / www.swlegal.sg

www.swlegal.ch

This Newsletter is available on our website www.swlegal.ch in English, German and French.