ATTORNEYS AT LAW

SCHELLENBERG WITTMER

FEBRUARY 2019

Newsletter

Authors:
Roland Mathys, LL.M. (LSE)
Andreas Hösli, LL.M.

ICT / WHITE-COLLAR CRIME AND COMPLIANCE

Response to cyberattacks - what needs to be done?

The risks posed by targeted cyberattacks on companies and their top management are constantly rising. While companies are increasingly aware of the risk exposure, uncertainty often exists relative to the action required, specifically whether the authorities (in particular specialized cyber prosecution authorities or the MELANI reporting office) should be involved in the event of an emergency.

1 CYBERATTACKS ARE A SERIOUS RISK

The press reports **cyberattacks** on nearly a daily basis. Cybercrime has become an attractive business model for increasingly professional perpetrators who often target **companies** and their **top management**.

Incidents that have become public, such as the severe impairment or even temporary paralysis of the IT infrastructure of numerous companies and public institutions, such as hospitals, through encryption software (e.g. *NotPetya*), have raised **awareness** of the problems at the management level. Nevertheless, the implementation of concrete counter-measures is occasionally lacking. In addition to massive **financial losses** (sometimes in the hundreds of millions) and severe **reputational damage** to the companies targeted, attacks on critical infrastructures can have serious consequences for entire societies. Further, there are justified concerns due to possible **fines** for data breaches (EU General Data Protection Regulation, **GDPR**). Accordingly, cyber threats pose **operational risks** which, if materialized, could threaten the very existence of companies. Cyber risks therefore require appropriate management. Given the dimension of possible damages, this is a **management task**.

2 CREATIVE ATTACKERS

The **attack methods** are manifold. In particular, attackers exploit IT security vulnerabilities (in software or hardware), insufficient passwords, and target humans as the "weakest link". Additionally, the generally low IT security of objects connected to the Internet (*Internet of Things*, e.g. security cameras) offers opportunities to attack. Common methods are Distributed Denial of Service (DDoS) attacks (flooding a system with very large amounts of data to overload and

temporarily paralyze it) or phishing (fraudulent obtaining of confidential data, e.g. by means of fake e-mails). The collection of unauthorized payments (allegedly on instruction of the management) has become known as CEO fraud. More recently, blackmailing has been increasingly observed, for example in the form of ransomware attacks, in which malware is used to encrypt foreign data or entire systems and a ransom (e.g. in the form of a cryptocurrency such as Bitcoin) is demanded for decryption.

> "Cyberattacks often target companies and their top management."

As outlined in our **February 2018 newsletter**, **prevention**, **action** and **response** are crucial to the legal management of cyber risks. However, there is considerable uncertainty within many businesses when it comes to the practical handling of the last aspect. In particular, when a cyber incident occurs, a question often arises as to whether a report to the authorities is appropriate or not, and who specifically should be contacted.

3 GENERALLY NO REPORTING OBLIGATION

In the event of a significant cyber incident, the company's (ideally existing) *Computer Security Incident/Emergency Response Team* (CSIRT/CERT) is responsible for taking the necessary immediate measures to mitigate damage and restore business continuity.

Apart from any *ad hoc* reporting obligations of listed companies and notification obligations for certain sectors based on special laws (e.g. for regulated financial institutions, telecommunications service providers or companies in the healthcare sector), a cyberattack currently triggers **no reporting obligation** to any Swiss authority. On the other hand, such a reporting obligation may arise in the event of **data protection violations** associated with a cyber incident under the GDPR and is also planned to be implemented in the amended Swiss Data Protection Act (**DPA**) currently under revision.

4 NOTIFICATION TO MELANI

Cyber incidents may be reported on a voluntary basis to the Reporting and Analysis Centre for Information Assurance (**MELANI**), a federal government agency, through its reporting form (www.melani.admin.ch). This may be done anonymously; however, anonymity makes it impossible for MELANI to reply. Such reports - around 8,000 per year - help MELANI develop a well-informed picture of the current situation regarding cyberattacks in Switzerland. MELANI also operates a platform through which **phishing activities** can be reported (www.antiphishing.ch), which regularly leads to the prompt deactivation of phishing websites in Switzerland. Independently of MELANI, art. 15 of the Ordinance on Internet Domains (OID) offers the possibility of blocking domain names via the registry operator (SWITCH) in the event of suspected misuse (in particular phishing and distribution of malware).

MELANI's mandate is primarily to protect and support selected **operators of critical infrastructures** (e.g. in the financial, energy, telecommunications and health sectors). To this limited group of participants, MELANI offers support in dealing with cyber incidents, in particular through technical analyses of its agency **GovCERT** (CERT of the Federal Government). In addition, MELANI enables confidential exchange of information with other operators of critical infrastructures. MELANI's services are generally unavailable (or available only on a *best-effort* basis) to other stakeholders (such as private individuals and SMEs that do not operate critical infrastructures; the scope of MELANI's activities is to be expanded in the future, see below). Notably, MELANI does not conduct any actual investigations; this is the responsibility of the law enforcement authorities.

5 INVOLVEMENT OF PROSECUTION AUTHORITIES

5.1 CRIMINAL PROSECUTION 2.0

Criminal prosecution in the digital space presents the authorities with new and major challenges. Cybercriminals operate very professionally, often from abroad and in the "darknet". In addition, numerous **new legal questions** arise, which await clarification by the highest court, e.g. in connection with the seizability of data.

> "Special cyber prosecution authorities have specific know-how."

In order to address the increasing movement of crime into the digital space, **dedicated cyber units** specifically charged with investigating cybercrimes have been organized in numerous Cantons as well as at the federal level. Since 2013, the Canton of Zurich has its own **Cybercrime Competence Centre** staffed with specialists from the public prosecutor's office and the police. This centre has a strong track record, including the restitution of stolen Bitcoins to damaged parties in several cases. In 2017, 240 proceedings were concluded, of which 23% by order of summary penalty order, 10% by indictment and 67% by closing order.

The **Office of the Attorney General** conducts several complex proceedings in its area of responsibility in connection with cybercrime. The Federal Criminal Police has its own IT Forensic/Cybercrime Department. Additionally, the Federal Office of Police (**Fedpol**) operates a platform through which suspicious cyber incidents can be reported (www.cybercrime.admin.ch).

5.2 CRIMINAL COMPLAINT

In the case of a serious cyberattack, companies should consider whether, in addition to the company's own mitigation efforts (e.g. as part of an internal investigation) and a notification to MELANI, the involvement of the **law enforcement authorities** is appropriate.

While the attacked company (or its CSIRT/CERT) focuses in particular on the defense against a (possibly persistent) cyberattack and the restoration of business continuity, the primary task of the law enforcement authorities is the **gathering of evidence** as well as the **localization and identification** of the suspected perpetrators. Among other things, this can be very helpful relative to the **restitution** of potentially stolen assets.

Criminal investigations in the cyberspace often involve **secret surveillance measures** (cf. art. 269 et seq. of the

Criminal Procedure Code, **CPC**; Federal Act on the Supervision of Postal and Telecommunications Traffic). One example is the collection of e-mails not yet retrieved by the account's user on the provider's server in the context of real-time monitoring.

As a rule, the chances of success of a criminal investigation are considerably higher if cyberattacks are reported **very promptly** after the incident. Cyber prosecutors are specialized in initiating investigations immediately in emergency cases. Ideally, they work closely with the IT specialists of the company concerned. As a rule, helpful **evidence** includes IP addresses and URLs, peripheral data, or log files relevant to the incident.

> "In most cases, there is no specific reporting requirement for cyber incidents."

Although reliable statistics are lacking, a **high number of unreported cases** of cyberattacks on companies can be assumed. On the one hand, not every attack is identified; on the other hand, many companies are reluctant to report incidents to the authorities, especially in view of possible **reputational damage**. If a criminal investigation leads to a court hearing, such a hearing is generally open to the public. Consequently, the company's sensitive information is at risk of disclosure. In addition, the criminal offences in question - such as computer offences (art. 143, 143bis, 144bis, 147 and 150 of the Criminal Code, CC), fraud (art. 146 CC), extortion (art. 156 CC) or economic espionage (art. 273 CC) - are in part *ex officio* offences that are investigated independently of the will of the reporting party. Understandably, companies may be reluctant to share sensitive information (e.g. regarding their own IT infrastructure) with outsiders. These reservations can be addressed by seeking **informal preliminary talks** with the public prosecutor's office wherever possible. For example, this may serve to clarify the prosecutor's office willingness to respect any subsequent declaration of disinterest by the company making the criminal complaint. In addition, the restriction of the right to inspect files in order to protect the company's legitimate interests in maintaining confidentiality (art. 108 CPC) should also be considered.

5.3 MUTUAL LEGAL ASSISTANCE 2.0

Due to the fact that cybercriminals often operate across borders, the chances of success of criminal investigations often hinges largely on the functioning of **mutual legal assistance** with other countries, which differs widely from country to country as experience shows.

In this context, the Council of Europe's *Convention on Cybercrime* (**CCC**, also known as the "Budapest Convention"), which came into force in Switzerland on 1 January 2012 and has also been signed by states such as the USA, Australia and Japan, is particularly relevant. One of the aims of the CCC is to facilitate legal assistance in the cyber area. In particular, art. 32 lit. b CCC provides for **direct access** to (or receipt of) data located in the territory of another Member State, provided that the prior **consent** of the person authorized to transmit the data in question has been obtained (e.g. a foreign Internet service provider who has reserved such a right vis-à-vis his customers in its data use guidelines). However, according to a decision of the Swiss Federal Tribunal, forced access (i.e. access without consent) by Swiss prosecution authorities to providers domiciled abroad is not permitted due to the **principle of territoriality**, given that international legal assistance in criminal matters is the designated pathway for this purpose (DFT 141 IV 108).

From the reverse perspective (access by foreign authorities to data located in Switzerland), the *Clarifying Lawful Overseas Use of Data Act* (**CLOUD Act**), which entered into force in the USA in March 2018, permits US law enforcement authorities to access data located outside the USA (via providers). Such access to data located in Switzerland potentially conflicts with art. 271 CC (prohibited acts for a foreign state).

6 OUTLOOK

Within the framework of the National Strategy for the Protection of Switzerland against Cyber Risks 2018-2022 (NCS II), the establishment of a **Cybersecurity Competence Centre** at federal level and a cyber force within the Armed Forces are core elements of Swiss government initiatives. The first strategic decisions in this regard were taken by the Federal Council at the end of January 2019. In particular, the mandate of MELANI is to be extended so that services can be offered for the entire economy and warnings and information can be issued to the public. In addition, the Competence Centre to be located at the Federal Department of Finance is to be given **powers of instruction** vis-à-vis other federal authorities to deal with cyber incidents. Further, the **introduction of an obligation to report** cyberattacks is likely to be examined, in particular with regard to operators of critical infrastructure. Finally, legislators in many other countries are currently very active in the field of cybercrime as well.

7 CONCLUSION

As digitization progresses, businesses (and individuals) must be prepared for the **risks posed by cyberattacks to increase further in the future**. In the event of an emergency, quick and decisive action must be taken. While notifications to MELANI are particularly useful for operators of critical infrastructures, the involvement of law enforcement authorities is an option to be seriously considered by any company (and individual) affected by a cyberattack, and one that needs to be examined very promptly.

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, LL.M. (LSE)
Partner
roland.mathys@swlegal.ch

Andreas Hösli, LL.M.
Associate
andreas.hoesli@swlegal.ch

In Geneva:

Louis Burrus
Partner
louis.burrus@swlegal.ch

Clara Poglia, MAS in Criminology
Partner
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
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.