



THE BIGGEST CYBER RISK: DANGER CAUSED BY HUMAN ERROR

Cybercrime can affect anyone – which means a well-prepared and carefully considered cyber policy is absolutely crucial for Swiss businesses.

Cybercrime is probably the most lucrative area of crime – and it's on the rise in Switzerland. The Swiss National Cyber Security Center (NCSC) received almost 50,000 reports of cybercrime in 2023 alone, a 30% increase on the previous year. Swiss authorities struggle to identify the perpetrators, who are often working from abroad, which is why only few are actually brought to justice. It is therefore up to potential victims, companies and private individuals in Switzerland to defend themselves against this threat.

Practical experience has shown that the greatest risk of falling victim to a cyber attack stems from the human factor, whether this involves employees, customers or own negligence. This Spotlight is intended to put the focus on these hazards and highlight the best ways to tackle the human factor. When it comes to criminal hacker attacks, you are not defenseless!

Prevention

Initial risk management begins with raising awareness and taking decisive preparatory steps. Establishing a meaningful prevention program is essential for pragmatic crisis management. The following aspects are particularly crucial to a well-functioning prevention program with regard to human factors:

- **Raising awareness:** Within the organization, all employees must be periodically informed of cyber risks and the right way to conduct themselves. A defense system is only as strong as the weakest link in the chain. In particular, it is important to raise awareness and promote vigilance with regard to phishing (the "fishing" of login data) and social engineering (attempts at identity fraud). Cybercriminals can fool almost anyone through social engineering – all should be aware of this.

One potential measure for directly raising awareness among employees is the sending of simulated phishing e-mails at irregular intervals by the company's own IT department, thus helping to expose vulnerabilities (i.e., careless individuals).

- **Define responsibilities:** It is extremely important to define key responsibilities in the event of a cyber attack. Every employee must be clear at all times on who they can turn to in the event of uncertainty or, in the worst case scenario, a cyber attack. This should also include the knowledge that employees should forward suspicious e-mails or external USB sticks to the company's internal IT department or external IT service provider for review. It is also important for private individuals to know that suspicious e-mails or files can be checked using free web tools (e.g. VirusTotal); caution should be exercised when dealing with confidential data.

- **Cyber incidents and crisis management directive:** It is also essential that the handling of cyber incidents and crisis management be defined as part of an employer directive. In this regard, particular attention should be paid to how and to whom employees must report cyber incidents immediately. The worst situation is when employees notice a cyber attack but don't know who to report it to internally and in what form. This means that valuable time is wasted – time attackers can use to harm the victim.

Crisis management also requires separate rules. It is important that employees who report cyber vulnerabilities or even attacks feel that they are being taken seriously. An appropriate whistleblowing or crisis management setup is indispensable. Otherwise, affected companies run the risk that dissatisfied employees prefer to talk to the press or third parties rather than to the relevant internal departments.

- **Cyber emergency protocol:** With the additional creation of a cyber emergency log for the event of a cyber attack, any redundancies in a crisis are eliminated effectively and profitably before the attack occurs. In particular, an emergency protocol of this nature should define the steps necessary to secure internal and external communication channels, including reporting obligations in order to contain a cyber attack and for the purposes of resuming operations. It is also worth specifying your existing contacts with external service providers such as IT experts, legal advisers or a communications agency for any press inquiries.
- **Insurance against cyber attacks:** If a cyber attack succeeds from the perpetrator's point of view, it necessarily involves costs and effort for those affected. Even successfully defending against a cyber attack without an outflow of money or data ties up resources and can be expensive. If insurance against cyber attacks has been taken out, it must also be noted that compliance with the reporting and mitigation obligations under the insurance contract is required. For this reason, too, it is essential to begin investigating the cyber incident immediately.

It must then also be checked whether insurance policies already taken out might also cover the occurrence of damage caused by cyber attacks.

EVEN THE BEST PRE-VENTION CANNOT COMPLETELY ELIMINATE THE POSSIBILITY OF A SUCCESSFUL CYBER ATTACK.

Response

Even the best prevention cannot completely eliminate the possibility of a successful cyber attack. It can only minimize the likelihood of it occurring. For a successful cybercrime defense system, it is therefore crucial that those affected have already acquired the knowledge and the responsive capabilities to deal concretely with a cyber attack. The following must be observed with regard to an adequate response to a cyber attack:

- **Ramp-up operation and documentation:** An appropriate response to a cyber incident naturally involves, as a first step, restarting operations and/or IT systems as soon as possible. In this respect, however, particular care must be taken to ensure that no evidence required for investigating the cyber attack is destroyed when operations are resumed. It is therefore worth documenting the impact of the cyber attack on IT systems and how the attack was dealt with from the outset. This ensures that a subsequent investigation and error identification is possible. Clear and comprehensible documentation is also necessary for reporting to the insurance provider.
- **Investigation and error identification:** Once the direct effects of the cyber attack have been eliminated, it is essential to investigate the incident and identify the (human) source of the error. This investigation can provide valuable insights that may prevent a repeat of a successful cyber attack of that nature. Such investigations are time-consuming and require large resources within a very short time. It is therefore often worth working with external partners on investigating the cyber incident.

An internal investigation and identification of the error source can then be used to determine whether the cyber directives issued earlier and the emergency protocol have been adhered to or whether the processes offer adequate protection in the first place. In the context of a subsequent criminal complaint, this allows key evidence to be produced at an early stage. Furthermore, this investigation can minimize liability risks for the management. This investigation and any error identification can also prove to the insurer that the victim is not at fault, which would minimize the insurance payout or even rule it out altogether.

- **Reporting obligations:** In order to minimize the liability risks of the company or management, it is necessary to check immediately whether there are any reporting obligations to the authorities or to customers. A cyber incident can trigger different official reporting obligations. If an incident poses a high risk to the privacy or fundamental rights of the data subject, it must be reported to the Federal Data Protection and Information Commissioner immediately¹. If a company is classified as a critical infrastructure, which is the case for banks, insurance companies and certain Internet service providers, among others, a report must be sent to the NCSC within 24 hours of a cyber attack². In return, organizations subject to the reporting obligation are entitled to support from NCSC in managing the cyber incident. If the company is subject to regulation by the Swiss Financial Market Supervisory Authority FINMA and the cyber attack is a critical one, a report must also be sent to FINMA within 24 hours³.

A cyber incident can also trigger an obligation to report to a customer or other data subjects. Data subjects must first be informed about an incident if they are (still) able to reduce the risks to their privacy or fundamental rights through certain measures, for instance, by blocking their credit card after a cyber attack on their bank.

Companies should answer the following questions in advance in order to be able to meet their reporting obligations in an emergency in a due and timely manner and thus minimize the risk of civil and criminal liability:

- What type of cyber incidents could trigger an obligation to report to the data protection officer?
- Is the company subject to a general reporting obligation to an authority, e.g. the NCSC?
- What information do we have to report to which authority in the event of an emergency and within what timeframe?
- **Ransom payment:** Paying a ransom in the event of a ransomware attack is an obvious option for many of those affected to get access to their data again quickly. Experience reports show that hackers often swiftly implement the promised concessions, such as unlocking servers, once the ransom has been paid, usually in cryptocurrencies. Hacking is a business model and hackers often operate in professional organizations that want to maintain their credibility. Victims therefore have – albeit very little – room for negotiation, as the attackers will only achieve their target if a payment is actually made. Note, however, that this involves dealing with criminals, which entails a certain degree of unpredictability in the overall situation. Important: All of this is not to say that a payment has to be made. The decision on whether a ransom payment should be made is a balancing of interests and an economic (and possibly emotional) appraisal of the potentially lost data. Alternative solutions, such as restoring from backups or working with cybersecurity experts, can be just as attractive and are probably more compatible with one's own sense of justice.

¹ Art. 24 para. 1 of the Data Protection Act

² Art. 74e para. 1 of the Information Security Act

³ FINMA supervisory notice on the obligation to report cyber attacks

- **Criminal complaint:** Irrespective of whether a ransom is paid, a criminal complaint should be filed with law enforcement authorities immediately. The police and the public prosecutor’s office often have enough technical and specialist human resources to prevent and investigate a cyber attack or, in the best case scenario, even to retrieve stolen assets or data. Subsequently, by initiating criminal proceedings, it is possible to secure evidence that is helpful for any claim report to the insurance provider. This evidence may also speed up the process of error identification and remedy any weaknesses in the victim’s processes.

The problems that companies and private individuals face in connection with cyber security and defense against cyber attacks are varied, challenging and by no means limited to technical issues. It is therefore worth seeking professional help at an early stage to build an effective defense system. After all, the perpetrators are also professionals at what they do.

Keyfacts

- 01 Cybercrime can affect anyone, so early preparation is crucial.**
- 02 Effective prevention requires raising awareness among employees, clear responsibilities and an emergency log.**
- 03 In the event of a cyber incident, rapid, well-considered action is essential in order to be able to quickly resume operations and secure evidence.**
- 04 Companies should review their reporting obligations and, if necessary, inform customers in order to minimize liability risks.**



Michael Mráz
Partner
m.mraz@wengervieli.ch
+41 58 958 53 18



Claudia Keller
Partner
c.keller@wengervieli.ch
+41 58 958 53 15



Loris Baumgartner
Associate
l.baumgartner@wengervieli.ch
+41 58 958 53 44



Matthias Langenegger
Associate
m.langenegger@wengervieli.ch
+41 58 958 53 43

Wenger Vieli is your reliable partner in legal and tax matters. Not only do we pride ourselves on bringing outstanding professional skills, experience, and a sense of responsibility to the table, but we are also highly inquisitive! Where others see obstacles, we see opportunities, find solutions, and open up new horizons. We do this with pleasure. In Switzerland, Europe, and the rest of the world.