PERSPECTIVES

HANDLING CYBER ATTACKS – HOW TO PREVENT, ACT ON AND REACT TO CYBER CRIMES

BY **DANIEL S. WEBER**
> WENGER & VIELI AG

The number of cyber attacks in Switzerland is on the rise and the problem is expected to get worse – both in terms of the volume and complexity of crimes being committed. Cyber attacks target almost all companies, regardless of industry, size or jurisdiction. The high and ever-growing dependency on and interconnectivity of information and communication technologies gives rise to pronounced vulnerabilities among Swiss companies.

For example, outages of and disruptions to IT systems resulting from cyber attacks can jeopardise the availability, confidentiality and integrity of critical services and functions. This can potentially go as far as cyber sabotage of critical infrastructure, or the disclosure of stolen information.

Moreover, attackers are becoming increasingly professional and well-organised. This makes it all the more important – but also more challenging – to prevent and combat attacks effectively. Cyber criminals not only have their sights on financial interests, but also target the availability, confidentiality and integrity of critical technology infrastructure and sensitive information.

Particularly in high-stress situations, such as the current coronavirus (COVID-19) pandemic, there is an increased risk of cyber attacks. Cyber criminals are utilising this time of uncertainty, adapting their attack strategies to the current situation and thereby

placing an additional burden on already challenged companies. In its yearly Risk Monitor report, the Swiss Financial Market Supervisory Authority (FINMA) considers cyber attacks one of the main risks for Swiss financial institutions.

Although companies are becoming more and more aware of the high risks associated with cyber attacks, there is often a lack of clear understanding as to what needs to be done to prevent and cope with this new form of threat.

This article discusses best practices in connection with preventing cyber attacks, immediate action to take in the event of an attack and how to the react in the wake of an attack.

Prevention of cyber attacks

The core of any defence strategy against cyber criminals is implementing measures to prevent cyber attacks from reaching their targets. Such measures are not only recommended to protect the company and its reputation, but are also partly required by law and should be embedded in a sound corporate compliance programme.

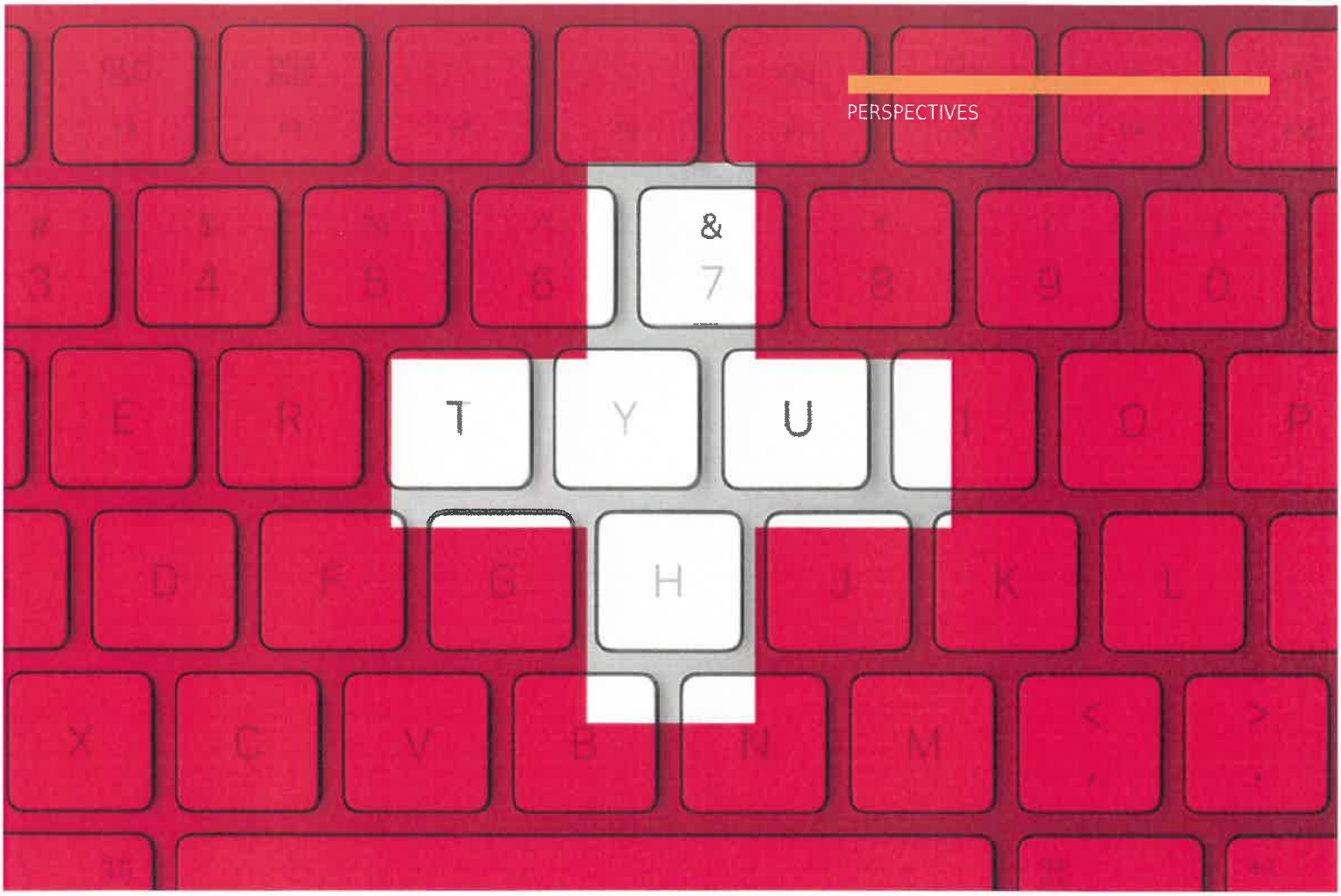
Swiss law does not impose specific obligations to prevent cyber risks. However, mitigating such risks is included in overall management responsibility and therefore is a duty of the board and management. The Swiss Code of Best Practice for Corporate Governance specifies that boards must ensure a risk management and internal control system adapted to the company. Given the current threat situation, preventing cyber risks is one of the key measures to be taken by the board.

Further, Swiss data protections laws – similar to the EU General Data Protection Regulation (GDPR) – state that personal data must be protected against unauthorised processing by appropriate technical and organisational measures.

Specific regulations on preventing cyber risks exist only in individual sectors, in particular in the financial services industry. According to FINMA's Circular 2008/21 'Operational Risks – Banks', boards must implement a risk management framework to address cyber risks. This must cover identification of specific threat potentials, protection of business processes and technology infrastructure, real-time detection and recording of cyber attacks, timely and targeted measures in response to cyber attacks, and appropriate measures to swiftly restore business operations following cyber attacks. Further, the effectiveness of these measures must be reviewed on a regular basis through vulnerability analyses and penetration tests.

First, it is recommended to establish a tailormade cyber security programme. This programme should define basic responsibilities, such as designating a chief information security officer (CISO). The programme should also set security standards to monitor systems to detect cyber attacks early.

Second, a company must identify the specific risks it is exposed to. An inventory of sensitive data and infrastructures should be drawn up as part of



this risk assessment. Possible threats and potential attacks should be identified, taking into account the human factor and potential for internal attacks. A solid gap analysis should then be used to identify gaps and weaknesses in the protection and defence system, and eliminate them with appropriate technical and organisational measures.

Third, the risk assessment should factor in the role of third parties. Providers of business-critical services should be subjected to thorough cyber security due diligence.

Fourth, employee training is a key element of preventive measures. On the one hand, training raises awareness of potential cyber threats. On the other hand, it provides employees with important principles for preventing cyber attacks and how to respond in the event of a successful cyber attack.

Finally, preparatory measures include developing a sophisticated cyber incident response plan with clear roles and responsibilities in the event of an attack.

Action in the event of an attack – cyber incident response

A company must prepare for an emergency. Even with best-in-class defence measures, it must expect a successful cyber attack. In addition to the quick detection of an attack, attention should be focused

on the correct conduct during an emergency, with detailed guidance provided, e.g., in a playbook.

Once under attack, the company's incident response team must act immediately. This team should include representatives from IT, legal & compliance, HR, communications and the business unit affected by the attack, as well as senior management. It should also include external specialists, including cyber forensic experts and lawyers.

The team must initially assess the severity and the impact of the cyber incident and take immediate action to minimise damage from a technical as well as reputational perspective. Business continuity must be ensured on short notice.

Then, the return to regular business operations must be initiated. The incident response team must also check whether and how the cyber attack is communicated internally and externally and whether formal notifications are required, e.g., to the regulator. Also, it must be decided if an internal investigation of the incident should be conducted and whether further steps, including criminal complaints or disciplinary measures, are warranted. Last but not least, the company should perform a root-cause analysis to learn why the attack was successful and what can be done to prevent it from happening again.

Reaction – notifications and legal action

If a successful or an unsuccessful cyber attack has occurred, the company must determine whether it needs to report the incident, and if so to whom.

"For listed companies, a duty to notify a cyber incident may arise from the rules on ad hoc disclosure. All information that is likely to have a significant impact on the company's share price must be disclosed."

A notification duty may arise under data protection laws. Under certain conditions and similar to the GDPR, the Swiss federal data protection and information commissioner and, if necessary, the affected individuals, must be informed 'as soon as possible' about a cyber incident.

In addition, there are different sector-specific reporting obligations, e.g., for service providers in the telecoms industry, for Swiss financial institutions such as banks and insurers, and in the health sector. For instance, FINMA published guidance in May 2020 to remind all supervised institutions of their legal requirement to immediately report any incident that is of substantial importance to supervisers. This

encompasses significant incidents with regard to successful or partially successful cyber attacks.

For listed companies, a duty to notify a cyber incident may arise from the rules on ad hoc disclosure. All information that is likely to have a significant impact on the company's share price must be disclosed.

Even if there is no statutory reporting obligation, a full disclosure may be advisable, e.g., for reputation reasons, best practice or to minimise potential damage. Once a cyber incident has occurred, the company must carefully evaluate if legal action should be taken against cyber criminals. Civil and criminal law remedies as well as individual special instruments are available.

From a civil law perspective, claims for injunctive relief, removal or damages may be based on breaches of contract or on tortious acts. In the latter case, illegality is usually based on a criminal offence being committed. Under criminal law, the possibilities include specific cyber crime offences, i.e., hacking, data theft or damage, computer fraud, as well as the regular criminal offences such as fraud, blackmail, coercion, forgery of documents or breach of secrecy. In Switzerland, there are several prosecution authorities at the state and federal level which specialise in investigating cyber crime.

Companies are also encouraged to report cyber incidents to the National Cyber Security Centre (NCSC) which is Switzerland's competence centre for cyber security and thus the first contact point for businesses, public administrations, educational institutions and the general public for cyber issues. Incoming reports will be analysed, but the NCSC is a technically oriented unit and not a law enforcement agency.

Conclusion – proactive management of cyber risks

Cyber security has become hugely important at all levels in recent years. It plays a key role in national and international foreign and security policy, and is increasingly an important factor for the general public and Switzerland as a business location. Therefore, the Swiss government has launched different initiatives in connection with cyber crime. These range from creating specific competence centres and centralised contact and coordination points, to introducing new reporting requirements, e.g., for operators of critical infrastructure.

In the wake of these developments, Swiss companies are becoming increasingly aware of cyber risks and realising that proactively managing cyber risks is a core element of corporate governance and compliance.

Daniel S. Weber
Counsel
Wenger & Vieli AG
T: +41 (58) 958 5858
E: d.weber@wengervieli.ch