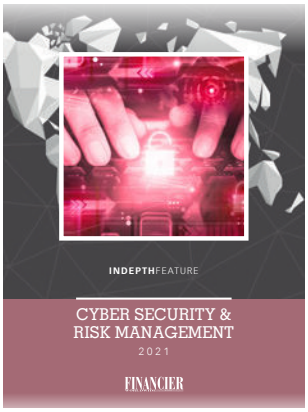

CMS Law.Tax

Published by Financier Worldwide Ltd

INDEPTH FEATURE Reprint April 2021

CYBER SECURITY & RISK MANAGEMENT

Financier Worldwide canvasses the opinions of leading professionals around the world on the latest trends in cyber security & risk management.

SWITZERLAND

CMS Switzerland

Respondent

DIRK SPACEK
Partner
CMS Switzerland
+41 44 285 11 11
dirk.spacek@cms-vep.com

Dirk Spacek is a partner at CMS who primarily deals with new business models arising in the media, internet and technology sector, data protection and intellectual property law. He mainly advises clients from the media, technology, industry and financial services sectors on technology-related legal matters and transactions.

CMS Switzerland

Q. In your opinion, what are the major cyber threats to which today's companies are vulnerable?

A: Multiple entry points for unauthorised breaches of corporate IT systems exist, and have existed for many years. These entry points can be used for various purposes by an attacker, such as damaging data or data systems, stealing data or using it as a means to extort money. As we have seen in recent years, there has also been a concerted effort to resell stolen data to foreign companies or foreign states. Sensitive personal data, including customer health or banking information, are particularly vulnerable to such attacks. Finally, complete system failures – so-called denial of service attacks – are particularly damaging. Not only do these threats create legal risks, they also involve reputational risks. Increasingly, companies are making use of third-party services, such as cloud offerings or external hosting providers, in which either their own IT systems are combined with or supplemented by other third-party providers. Since every third-party provider is also a gateway for potential service disruptions, contractual third-party management is an important pillar of mitigating cyber risks.

Q. Given the risks, do you believe companies in Switzerland are placing enough importance on cyber security? Are board members taking a proactive, hands-on approach to improving policies and processes?

A: For many large companies, cyber security is a top management item on their agenda, with significant resources allocated toward it. Smaller companies with fewer resources available might not invest as much. Regardless of the resources dedicated to cyber security, IT security risk management is considered the legal obligation of each company's management team. Thus, they must create an IT risk management framework and regularly review the vulnerability of their IT systems. This emanates from corporate law principles and is also set forth in corporate governance guidelines in Switzerland. In highly regulated sectors, such as the financial services industry, increased regulatory requirements with a bearing on IT security apply.

CMS Switzerland

Cyber attacks are punishable under criminal law statutes in Switzerland, but law enforcement can be difficult as perpetrators are often hard to trace.

Q. To what extent have cyber security and data privacy regulations changed in Switzerland? How is this affecting the way companies manage and maintain compliance?

A: The current Swiss Federal Act on Data Protection (FADP) has been subject to comprehensive revisions in recent years. This has been triggered by new standards established under the EU General Data Protection Regulation (GDPR) and an attempt by the Swiss government to harmonise with these standards. The new, revised statute is expected to enter into force in mid-2022 and will be closely aligned with the GDPR, albeit still slightly more liberal. Like the GDPR, the new FADP will introduce sanctions for non-compliance with data protection obligations and have a deterrent effect on companies, even though they will be lower than in the EU – a maximum of 250,000 Swiss francs and, unlike in the EU, qualify as criminal sanctions, which must meet high thresholds to enforce, and not administrative sanctions. While IT security is already a mandatory obligation for data controllers under the current Article 7 FADP, the new FADP will introduce

CMS Switzerland

so-called 'data breach notification duties' requiring parties to notify supervisory authorities and the data subjects affected by data breaches under certain circumstances. All of this will certainly increase the pressure on companies to apply solid IT security management to any personal data stored and processed by them. Proactive data privacy management will therefore become a vital pillar in company management.

Q. In your experience, what steps should companies take to avoid potential cyber breaches – either from external sources such as hackers or internal sources such as rogue employees?

A: Cyber attacks are punishable under criminal law statutes in Switzerland, but law enforcement can be difficult as perpetrators are often hard to trace. It is therefore not enough to rely solely on the legal apparatus of public authorities. Comprehensive and proactive early detection and countermeasures – so-called 'computer forensics' – are suggested. As part of an IT security programme, employees should also be trained to recognise the potential dangers of cyber attacks. Regarding rogue employees, this is a more delicate matter. Only if there are reasonable indications of misuse or suspicious behaviour can monitoring activities be justified. Surveillance activities should usually be announced and systematic surveillance of employees is generally forbidden under Swiss data privacy and under employment law statutes.

Q. How should firms respond immediately after falling victim to cyber crime, to demonstrate that they have done the right thing in the event of a cyber breach or data loss?

A: We recommend seeking immediate legal advice on urgent notification duties. Such notification duties can arise under the future FADP, but also based on obligations established in existing customer contracts. Under data privacy law standards and contractual considerations, it is pertinent to document the findings gathered on the attack, a root-cause analysis of the weakness in the system and measures should be taken to avoid similar attacks in the future. By this means, it is evidenced that a company has responded with

CMS Switzerland

adequate care and diligence to a threat. Another question to be carefully assessed is whether ransom payments should be made or not.

Q. In what ways can risk transfer and insurance help companies and their D&Os to deal with cyber risk, potential losses and related liabilities?

A: The risk of cyber attacks exists and cannot be erased. Insurance solutions offer financial compensation for losses and often bear costs for technical and legal experts. Smaller companies might benefit from such knowledge and assistance whereas large companies might have sufficient expertise in-house. Nonetheless, the most effective way to deal with cyber risks is prevention and pre-emption. While we have seen cyber risk insurance offered in Switzerland, it is not yet widespread.

Q. What are your predictions for cyber crime and data security in Switzerland over the coming years?

A: Awareness of cyber crime and data security issues will increase. Not only will they be considered a general management topic, but more importantly, they will become an important pillar of data privacy management, especially under the revised FADP. We also presume that contract management with third party IT providers will be subject to closer scrutiny, since companies want to ensure that they investigate their risks appropriately. ❑

CMS Switzerland

www.cms.law

CMS operates in 43 countries and 77 offices worldwide. The firm's 4800 lawyers offer business-focused advice tailored to individual needs, whether in local markets or across multiple jurisdictions. Being immersed in the industry sectors its clients operate in is at the heart of what CMS does. The firm is structured according to the industries its clients work in, delivering technically excellent lawyers who talk clients' language.

DIRK SPACEK Partner
+41 44 285 11 11
dirk.spacek@cms-vep.com

C/M/S/
Law.Tax