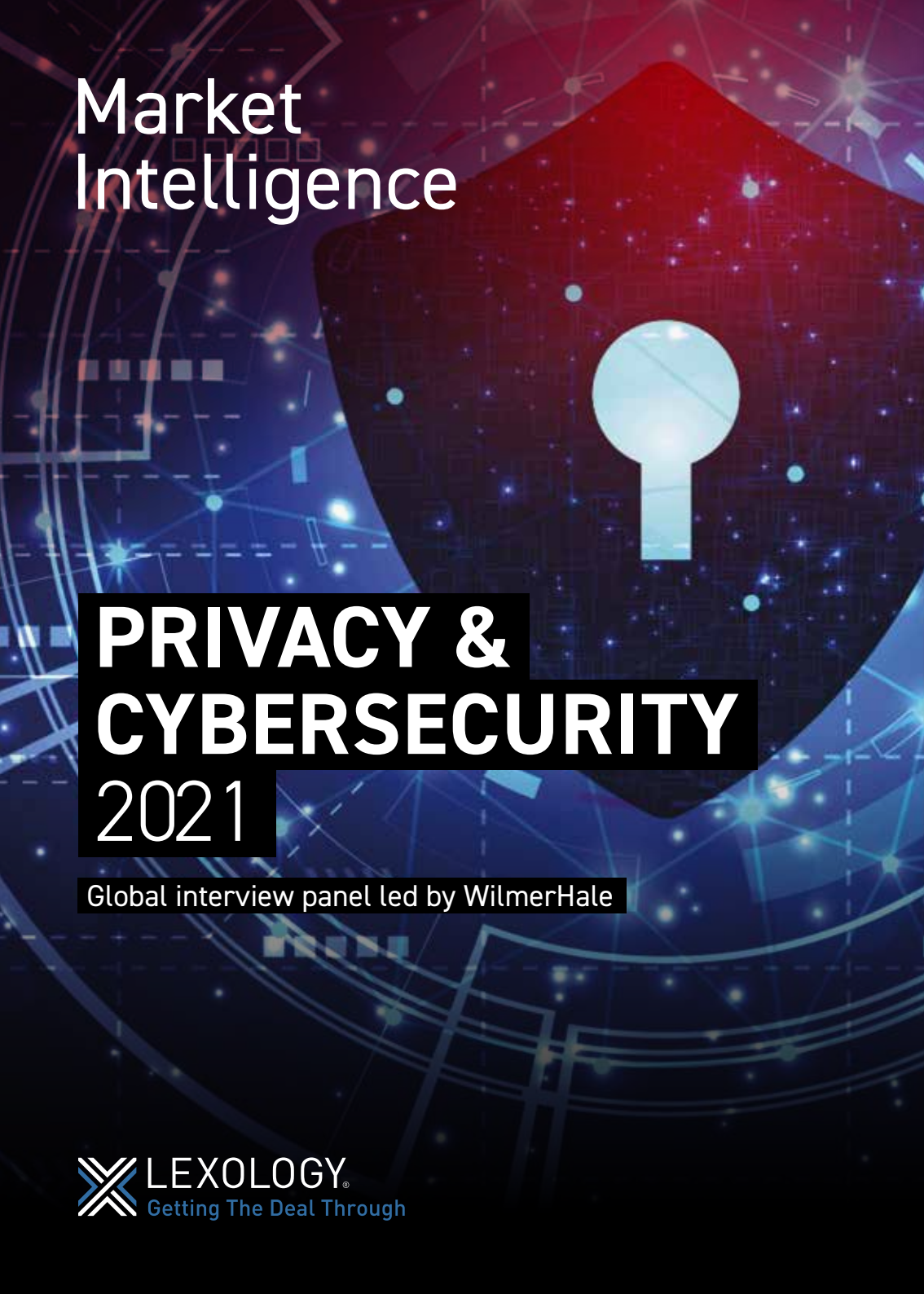


Market Intelligence

PRIVACY & CYBERSECURITY 2021

Global interview panel led by WilmerHale

LEXOLOGY®
Getting The Deal Through

LEXOLOGY
Getting The Deal Through

Publisher
Edward Costelloe
edward.costelloe@lbresearch.com

Subscriptions
Claire Bagnall
claire.bagnall@lbresearch.com

Head of business development
Adam Sargent
adam.sargent@gettingthedealthrough.com

Business development manager
Dan Brennan
dan.brennan@gettingthedealthrough.com

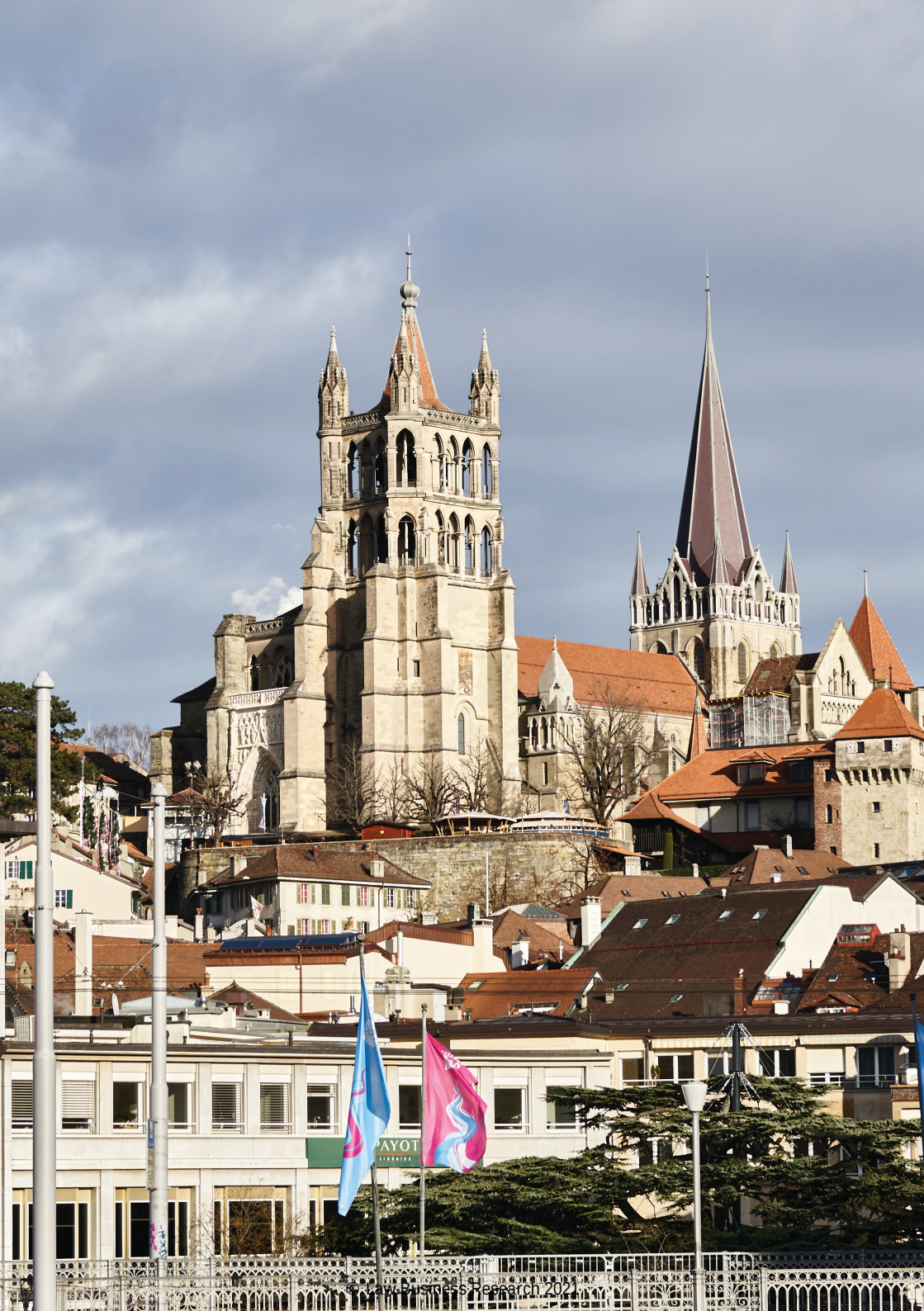
Published by
Law Business Research Ltd
Meridian House, 34-35 Farringdon Street
London, EC4A 4HL, UK

Cover photo: shutterstock.com/g/Chor+muang

ISBN: 978-1-83862-740-9

Printed and distributed by Encompass Print Solutions

Privacy & Cybersecurity 2021



Switzerland

Jürg Schneider is a partner at Walder Wyss and the head of its Lausanne office. His practice areas include information technology, data protection and outsourcing. He regularly advises both Swiss and international firms on comprehensive licensing, development, system integration, and global outsourcing projects. He has deep and extensive experience in the fields of data protection, information security and e-commerce, with a particular focus on transborder and international contexts. In addition, Jürg Schneider regularly publishes and lectures on ICT topics and is a member of several professional organisations.

David Vasella is a partner on the information technology, intellectual property and competition team at Walder Wyss. He advises and represents Swiss and international companies in all industries and at all stages of growth on questions concerning data and technology law. He specialises in data use, negotiating data-related contracts, data security issues, cloud projects and IT contracts and provides support in setting up platform models and data protection compliance in accordance with GDPR and Swiss law. He regularly gives talks and writes publications on his areas of expertise, for example on datenrecht.ch, a Swiss platform on data law.

Hugh Reeves is a managing associate in the information technology, intellectual property and competition team at Walder Wyss. He advises clients in matters of technology transactions, commercial contracts, telecommunications, intellectual property and digitalisation. In addition, he is active in the areas of data protection as well as e-commerce and assists clients with their entry or expansion in the Swiss market.

1 What were the key regulatory developments in your jurisdiction over the past year concerning cybersecurity standards?

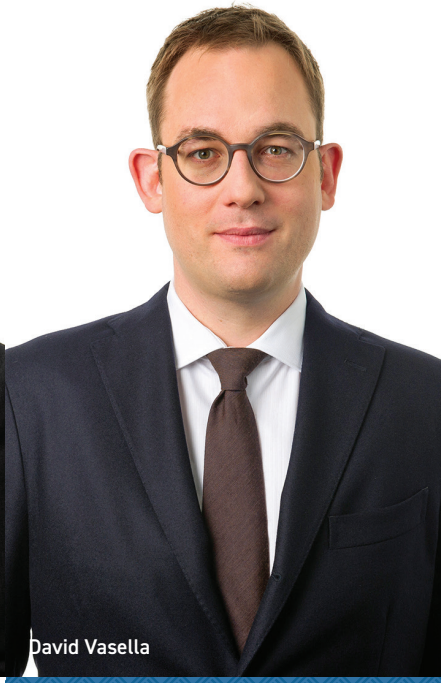
Swiss laws and regulations typically steer away from using specific technical standards. The reason for that is the legislator's (Parliament's) policy decision to draft laws on a technologically neutral basis, unless the nature of the law would make that impossible. Because Switzerland is a civil law country, and because our legislative process is comparatively slow, the inclusion of technical standards into the laws would risk rendering the laws obsolete or overly rigid.

Instead of relying on specific technical standards, current Swiss laws typically refer to more abstract concepts such as the 'state of the art'. This is the case for cybersecurity. Local laws still mostly address cybersecurity as a subset of data security, which in turn is a component of data protection legislation. As per legal requirements, data security calls for technical and organisational measures that must be 'appropriate' and 'suitable' to achieve certain security goals such as transport, storage and access controls.

Parliament recently overhauled data protection legislation. The new law is tentatively scheduled to enter into force in 2023, as a consequence of the above-mentioned moderately paced legislative process. Despite some initial discussions on the topic of the inclusion of specific standards, the revised law will not contain more detailed requirements.

The general absence of regulatory requirements concerning cybersecurity standards might seem surprising. Businesses do sometimes struggle with the current legislation, as it requires 'adequate' measures but remains mute on what that actually, technically, means. This is particularly true for companies working with new technologies such as distributed ledger technologies (or blockchains), which have not been fully assessed from a legal perspective and are not discussed in frequent court decisions. Rather, the federal government has looked to strengthen its administrative capabilities, by setting up an overarching National Cybersecurity Competence Centre (NCSC) to assist the various market actors with the challenges posed by cyberthreats and enable a coordinate response thereto. The government has also been implementing several 'National Strategies for the protection of Switzerland against cyber risks' (NCS), which recommend a mix of legal and technical solutions towards cybersecurity.

As a result, there is growing awareness within the private sector of cybersecurity and the absence of clear regulatory cybersecurity standards has arguably not prevented companies from pursuing a high level of cybersecurity. Indeed, the main obstacle would appear to be a financial one, rather than a legal one. SMEs are the prevalent structure in the Swiss private sector landscape and an occasional lack of



"There is growing awareness within the private sector of cybersecurity."

awareness around cyber risks, combined with limited budget allocations thereto, appear to be the main culprit behind weak cybersecurity measures.

At the intra-governmental level, the situation is overall comparable. After one whole decade of stop-and-go legislative talks, Parliament approved (in December 2020) a draft Information Security Act. This draft act seeks to govern information security measures within the federal administration and imposes various requirements around information security practices. However, it shies away from any reference to technical cybersecurity standards, again as an implementation of the technological neutrality policy.

Overall, we are favourable to a technologically neutral legislative agenda. It generally works well with Swiss laws, which are, by design, mostly worded as general rules and allow the market to implement dynamic and creative solutions. The drawback is a lack of predictability. So far, in the area of cybersecurity, this has not been a major cause for concern, because companies are usually able to reach legal compliance simply by following general market practices. As new technologies hit the market, however, we do expect that more technical legislation will become necessary in the coming years. Such legislation will not be needed as a general obligation (such as data protection), but should rather target specific industries or technologies, such as critical infrastructures or cloud storage technologies. An explicit reference, in the laws, to accepted standards or certifications as a minimum requirement would also help smaller companies navigate their way towards adequate cybersecurity measures.

2 When do data breaches require notice to regulators or consumers, and what are the key factors that organisations must assess when deciding whether to notify regulators or consumers?

Breach notification has been an ongoing topic in Switzerland. As of now, and with a few sector-specific exceptions, there are not any express breach notification obligations. However, in certain cases, such notification obligations may implicitly ensue from the principle of transparency under data protection legislation or a contractual obligation. This being said, this will change with the revised data protection act, set to enter into force in 2023.

Under the text of the revised data protection act, data controllers will have to notify the data protection authority 'as soon as possible' of any data security breaches that are likely to result in a high risk to the personality rights or fundamental rights of data subjects. Data processors will have to notify the controllers of 'any data security breach'. Data subject notification, however, will be reserved to situations where the notification is 'necessary for the protection' of the data subject or upon request of the data protection authority.

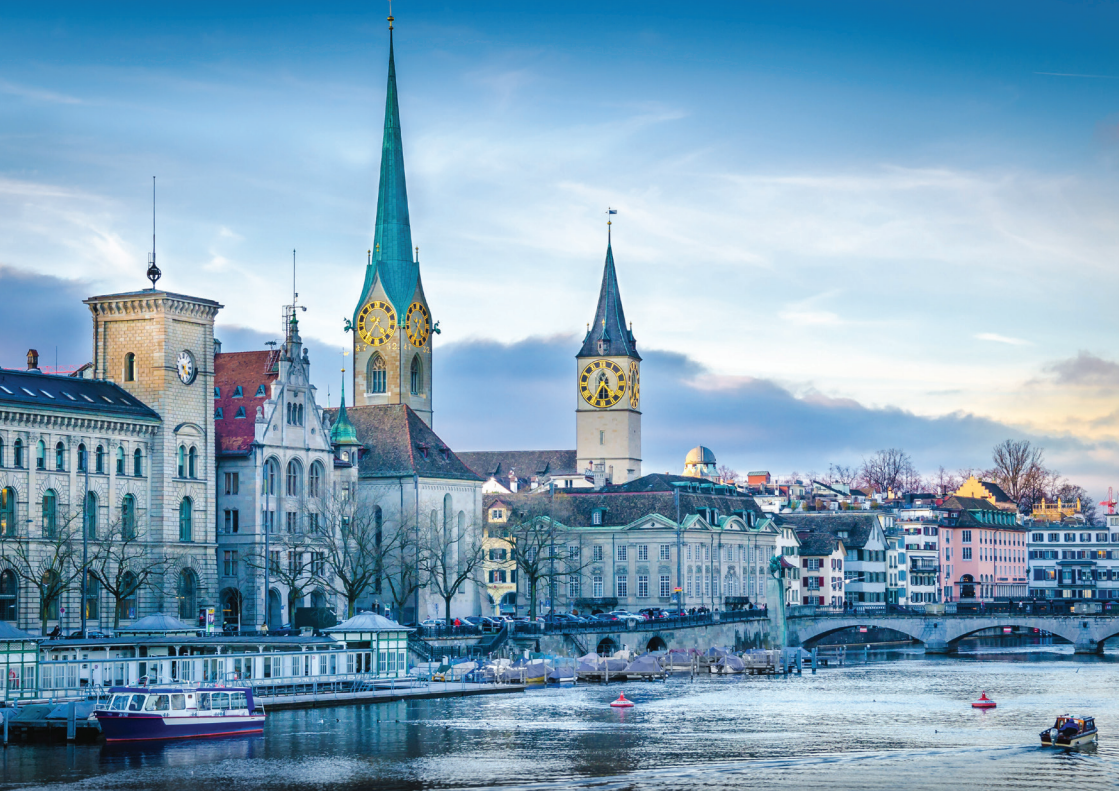


Photo by Alexandru Staiu on Shutterstock

In addition, the government has been seriously contemplating specific breach notifications in the case of critical infrastructure (which includes energy grids, water supplies, transport and communications). It was indeed felt, in the course of the NCS, as mentioned in question 1, that the absence of clear reporting obligations could jeopardise the proper functioning of critical infrastructures and hinder adequate responses in case of a cyberattack.

Despite the absence of general express breach notification obligations, we notice, in practice, that companies who have fallen victim to cyberattacks or other forms of data breaches frequently go public with the news. This is due, on the one hand, to the fact that many Swiss-based companies also process data of European Union or European Economic Area residents or fall under the scope of the General Data Protection Regulation (GDPR) for other reasons and, on the other hand, that many data breaches become public knowledge rather quickly. This latter scenario results in additional reputational harm on the company suffering the breach, as it leads the public to believe that said company was hoping to hide the event rather than be transparent. In that sense, breach notification is not solely dictated by legal provisions, but also – perhaps even more so – by reputational ones. Therefore, any

"Strong technical measures and organisational measures give companies a lot of peace of mind."

organisation considering a breach notification should factor in the reputational elements in deciding whether to report the breach and the extent of any publicity surrounding the breach notification.

3 What are the biggest issues that companies must address from a privacy perspective when they suffer a data security incident?

Apart from mitigating the risk of reputational harm, as mentioned in question 2, which is not strictly a privacy issue, the main issues are twofold.

First, organisations must rapidly identify the origins and scope of the data security incident. What we mean by that is that companies should really allocate sufficient resources to obtaining all information possible on the full chain of events that led to the incident. This is an essential task, as it will then allow the company to decide how to respond, what corrective measures it needs to implement, how to allocate responsibilities (internally or with involved third parties such as storage providers) and so forth. It also will allow the company to determine if the incident is

still ongoing, as may be the case if an ill-intentioned actor revealed a backdoor in the company's IT systems and shared those revelations on the darknet.

Secondly, but at the same time, organisations have to know as quickly as possible if the incident impacted any data, such as personal data and confidential information, affecting its contractual partners, such as customers or research partners. Failure to do so could have grave repercussions on the company's business and may result not only in a loss of customers, but also in complaints of violations of data protection legislation and of contracts. Indeed, many contracts include, for instance, penalties in case of breaches of confidentiality. These provisions likely rarely apply to situations of data security incidents, but if they do, the amounts (in addition to any damages) could quickly add up.

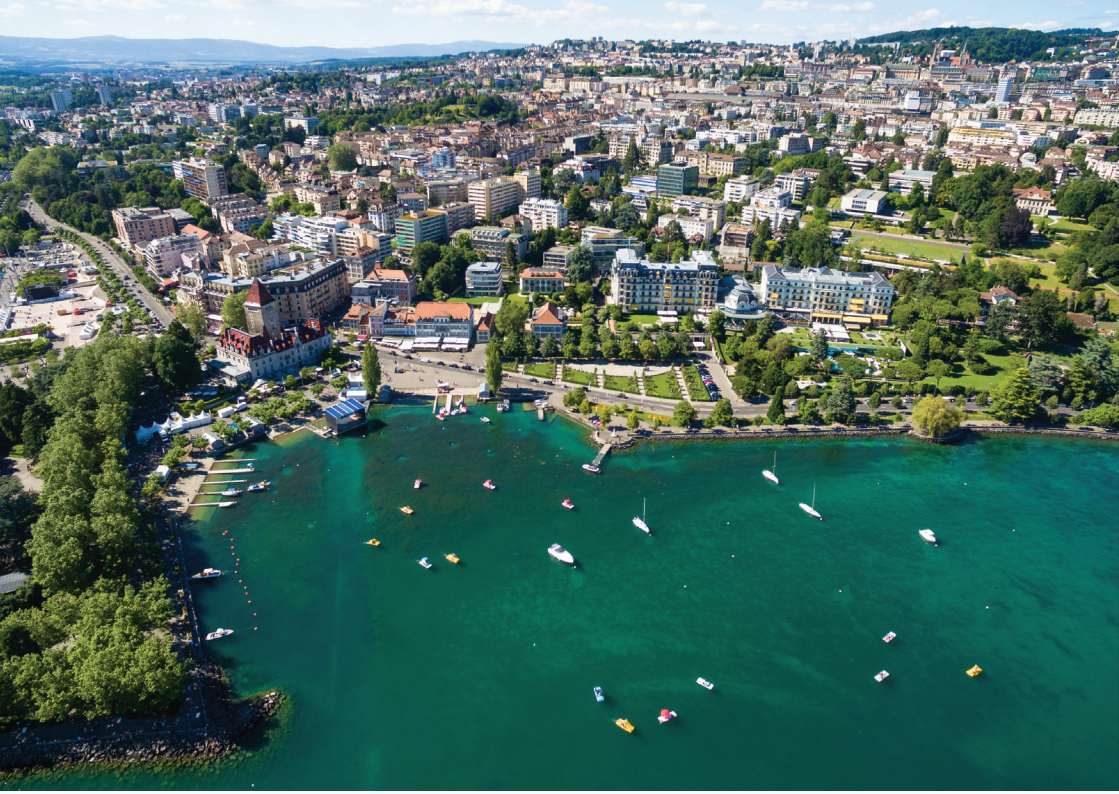
We can also note that it is important for companies to have written policies explaining the steps the company should take in the case of a data security incident. Such policies are now commonplace, though their quality varies. In any case, we do encourage companies to have such policies in place, even if the policy is very basic. Indeed, situations of security incidents call for extremely rapid responses and even the most general of roadmaps will go a long way in helping the company's management to react.

4 What best practices are organisations within your jurisdiction following to improve cybersecurity preparedness?

Preparedness is indeed the key word. Strong technical measures, such as a resilient IT backbone, and organisational measures, such as adequate internal policies dictating responses to cyber-risks, give companies a lot of peace of mind.

In addition, we believe a lot of the preparedness should focus on awareness and training. Still, today too few companies fully comprehend the seriousness of cyber-risks and their potential impact. Cyberthreats have become highly sophisticated and can fully incapacitate even well-prepared organisations. Moreover, the potential financial harm in case of a theft of trade secrets and other sensitive information is staggering. Companies should therefore seek to raise awareness among their staff, starting with the management, and then implement regular internal training as well as hiring trusted providers to test the company's resistance to cybersecurity threats.

In particular, we note that, despite the sophistication and power of some recent cyberattacks, many companies fall victim to cyberattacks via simple phishing. This is where, for instance, employees open a compromised file sent to them in an otherwise harmless-looking email. This can quickly result in the sharing of passwords and login credentials, which hackers can easily use to their advantage.



A less talked about topic is cyber-risk insurance. Many insurance providers now offer insurance coverage for cyber-risk events. Somewhat amusingly, anecdotal evidence seems to suggest that some companies see such insurance policies as a frontline defence against cyberthreats. This is a risky gamble. Despite all the qualities of such insurances, they cannot replace a proactive and careful approach towards cybersecurity.

The bottom line here is that any organisation should regularly read reports of the above-mentioned NCSC, ensure it has a competent IT team either in-house or as an external service provider and provide ongoing training and awareness events for its staff. The use of external services such as bug bounties and penetration testing is also highly advisable in many cases, especially when a company is implementing new software or upgrading its IT systems.

Photo by Samuel Borges Photography on Shutterstock

5 Are there special data security and privacy concerns that businesses should consider when thinking about moving data to a cloud hosting environment?

The use of cloud hosting is quite ubiquitous. Arguably, using third-party cloud providers can, in many cases, lead to a higher level of data security than relying on an internal IT storage set-up. This is primarily because of pure specialisation. Cloud providers often have decades of experience in the hosting area, whereas their clients may be active in a radically different area and have not been able to remain up-to-speed with technological evolutions in the hosting and IT security landscape.

Therefore, data security is rarely a sticking point when relying on cloud service providers and the discussions between the parties rather revolves around business continuity, key performance indicators, support levels and so on. That said, this is assuming the cloud service provider is trustworthy and capable.

Privacy, on the other hand, remains a very real concern. This is, in part, due to the end of the Privacy Shield framework (both for Switzerland and for the EU in relation to the United States). As a result, cross-border data flows, and 'offshore' data storage in the United States could qualify as a breach of Swiss (and EU) data protection legislation, due to the absence of proper safeguards surrounding the disclosure of personal data abroad.

In the same way, telecommunications surveillance legislation often – as is the case in Switzerland – empowers the government to obtain access to information at certain conditions. In the case of Swiss telecommunications surveillance legislation, the criminal investigation authorities can, under certain conditions, obtain information stored in or controlled from Switzerland. Perhaps counter-intuitively, such information requests may target providers of cloud hosting services. Indeed, though such service providers do not directly provide telecommunications methods, the storage of information is a relevant trigger under Swiss telecommunications surveillance legislation. In fact, it is these same considerations that led to the downfall of the Privacy Shield framework.

For all those reasons, businesses should not shy away from transferring data to a cloud hosting environment, because cloud service providers often are able to provide higher quality at a cost equivalent or better to what many companies could obtain if they dealt with storage internally. These businesses should, however, carefully assess the type of data they intend to transfer to the cloud, as well as the technical nature of the transfers and the storage (ie, encryption to data in transit or at rest). Lastly, the jurisdiction in which the cloud servers are located plays a key role and, for that reason, many organisations choose a provider with local servers.

"The setting-up of the NCSC, incorporating pre-existing governmental cybersecurity bodies, has been a big step in the right direction."

6 How is the government in your jurisdiction addressing serious cybersecurity threats and criminal activity?

The Swiss government has been focusing particularly on cybersecurity. It assesses the Swiss cybersecurity landscape on a continued basis, by means of the NCS, mentioned in question 1.

The most important result in our view has been the remarkable increase in awareness. Arguably, Swiss companies (and individuals) had become rather complacent. As is often the case, many believed that cyberattacks only happened to others. Therefore, when the government shone the spotlight on the increase in cyberthreats, together with some highly mediatised cyber incidents affecting important Swiss market actors, we noticed a rapid shift in standard business processes.

The setting-up of the NCSC, incorporating pre-existing governmental cybersecurity bodies, has been a big step in the right direction because it is staffed with highly skilled experts and enjoys a strong credibility on the market.

Other initiatives, such as the private-public Trust Valley ecosystem, look to capitalise on Switzerland's status and experience in the cybersecurity and internet

area. They provide an environment that allows public and private actors to discuss and, in the best of cases, to find solutions to current or future cyberthreats.

7 When companies contemplate M&A deals, how should they factor risks arising from privacy and data security issues into their decisions?

M&A deals are truly multifaceted as they involve many legal considerations. We can highlight the following.

From the selling company's perspective (ie, the company that should be acquired at the end of the deal) it must be kept in mind that, in the near or medium future, its data will often be stored with the acquiring company's data (meaning on common servers or with a common provider). Indeed, the buyer will rarely be interested in relying on separate IT systems or on separate hosting providers, because doing so would not only increase costs, but would complicate the management of the IT systems and data storage. Even in the case of fully separated data storage, the acquiring company will usually and eventually have the right to access all the selling company's data, by simple virtue of being the owner or majority shareholder of said selling company. This is true in particular in the case of 'share deals'. In the case of 'asset deals' where there is no change of hands of the shares and the rights attached thereto, the situation can be comparable – or even more drastic – as the transferred assets may include data sets. The selling company will also need to ensure that it may disclose certain information, such as employee names, during the due diligence process leading up to the M&A deal, as failing to do so could give rise to liability in particular under data protection law.

Though the concerns raised above are often harmless in practice, such deals could have a negative impact, at least to reputation, for a selling company that built its reputation, for instance, on outstanding data security or on storage solely in a given jurisdiction (as is frequently the case). The selling company should therefore carefully consider this point and determine if it wishes to risk its hard-earned market reputation.

From the buyer's perspective, data security issues are a hot topic. Indeed, a data breach could involve the loss of valuable trade secrets, such as secret recipes, client lists, production methods and so forth. Moreover, the reputation harm frequently associated with (publicised) data breaches not only risks spreading to the buyer but also may reduce the market value of the selling company's trademarks as well as its market valuation. As an example, publicly traded companies tend to experience a noticeable dip on the stock market if they suffer a cybersecurity event. Also, under the GDPR, data privacy breaches may lead to high fines. As these fines are calculated on the entire group turnover, acquiring a company that is still breaching

privacy rules could have an even higher financial impact. For this reason, conducting an extensive privacy and data security due diligence is of essence in any M&A deal. Of course, data protection in general is an important topic as well, because the buyer will want to ensure that it can use the data for its business after the deal. This would be difficult or even impossible if such data was not lawfully collected, for instance.

Jürg Schneider
juerg.schneider@walderwyss.com

David Vasella
david.vasella@walderwyss.com

Hugh Reeves
hugh.reeves@walderwyss.com

Walder Wyss Attorneys at Law
Lausanne and Zurich
www.walderwyss.com

The Inside Track

When choosing a lawyer to help with cybersecurity, what are the key attributes clients should look for?

Cybersecurity is very much an area where experience is necessary. This said, clients should ultimately base their choice on personal preference. When dealing with cybersecurity, a lot of the underlying information is highly sensitive and the client–attorney relationship will need to rely on the highest level of trust in order for it to bear fruit.

What issues in your jurisdiction make advising on cybersecurity and privacy complex or interesting?

Firstly, the relevant technologies are evolving very rapidly. We enjoy following technological evolutions and catching a glimpse of tomorrow's technologies. Secondly, we are frequently dealing with international matters. This multinational context is rife with complexities but is, for that very reason, a real pleasure to work with.

How is the privacy landscape changing in your jurisdiction?

At the time it was passed in 1992, Switzerland's data protection act was particularly modern and helped Switzerland secure its position as a hub for data security and confidentiality. In September 2020, Parliament signed off on a fully revised data protection act. This new law is going to bring closer alignment to the EU's GDPR. We are also following with a lot of interest the public dialogue around privacy. These are reflected in the discussions surrounding telecommunications surveillance, which often boils down to strong privacy prerogatives versus governmental access to personal information for security purposes.

What types of cybersecurity incidents should companies be particularly aware of in your jurisdiction?

Ransomware and attacks aiming at the theft of trade secrets are two types of incidents which require constant and high awareness. That said, companies need to evaluate their cybersecurity worst case scenario individually. Even though companies can evaluate cyber-risks on a general level, they are also right to keep in mind that their situation is always unique and requires a tailored approach.

Lexology GTDT Market Intelligence provides a unique perspective on evolving legal and regulatory landscapes.

Led by WilmerHale, this *Privacy & Cybersecurity* volume features discussion and analysis of emerging trends and hot topics within key jurisdictions worldwide.

Market Intelligence offers readers a highly accessible take on the crucial issues of the day and an opportunity to discover more about the people behind the most significant cases and deals.

Covid-19 response
M&A risks
Latest regulatory trends
Cloud hosting

an LBR business

ISBN 978-1-83862-740-9