Photo byMichael Traitov on Shutterstock

LEXOLOGY
Getting The Deal Through

Market Intelligence

PRIVACY & CYBERSECURITY 2023

Global interview panel led by WilmerHale

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.

Post-covid trends
Cloud hosting
M&A risks
Selecting counsel

START READING

About the editors

Jason Chipman
WilmerHale

Jason Chipman is a WilmerHale partner who advises companies on complex regulatory matters associated with data security, cyber incident response, the Committee on Foreign Investment in the United States and related export controls.

Benjamin Powell
WilmerHale

Benjamin Powell is a WilmerHale partner who has advised companies on major cybersecurity incidents and preparedness across virtually every sector, including banking, investment management, retail, defence and intelligence.

Arianna Evers
WilmerHale

Arianna Evers is a WilmerHale special counsel who advises clients on complex privacy, data security and consumer protection issues.

Shannon Togawa Mercer
WilmerHale

Shannon Togawa Mercer is a WilmerHale senior associate who advises clients on matters related to cybersecurity, privacy, and US and European data protection.

Contents

While reading, click this icon to return to the Contents at any time

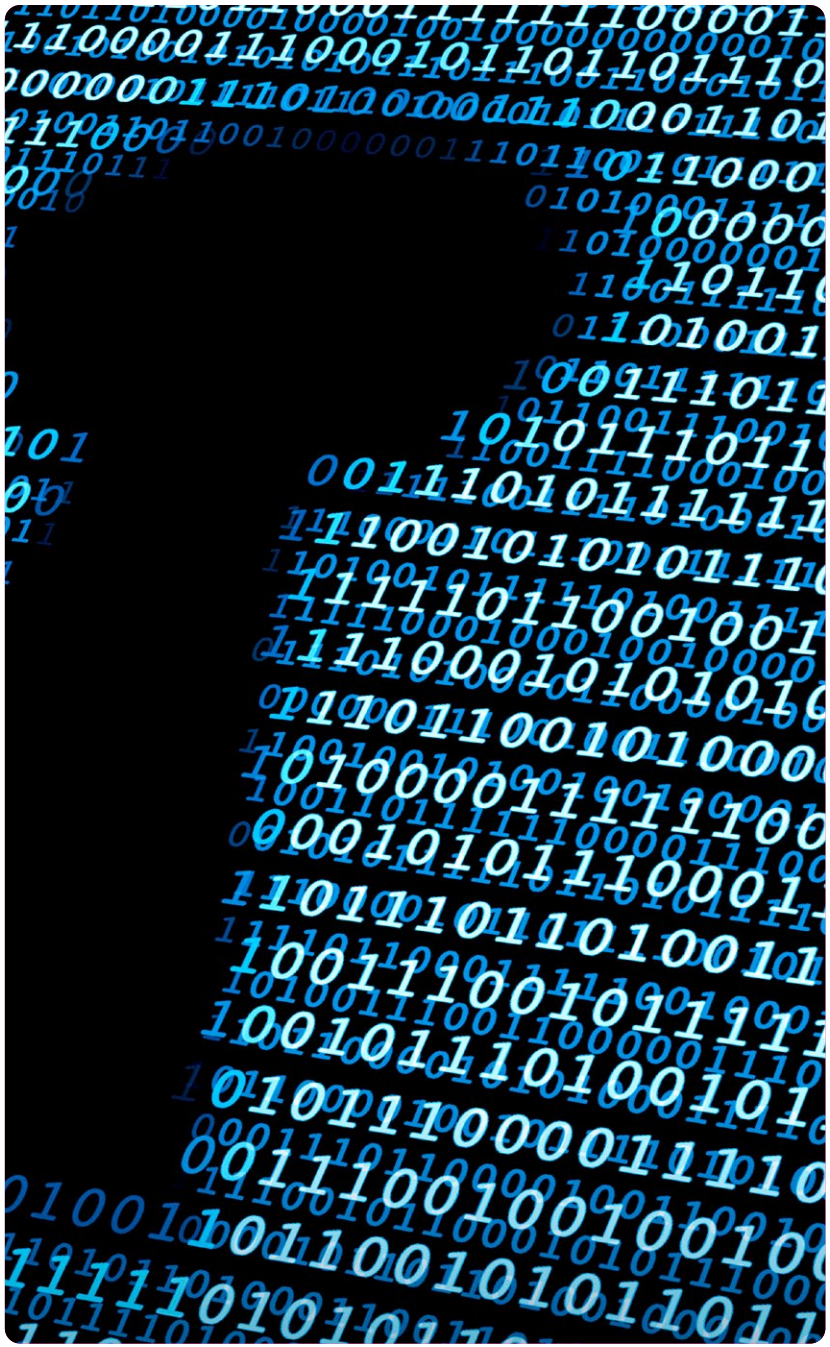


Photo by enzozo on Shutterstock

Global trends

Jason Chipman is a WilmerHale partner who advises companies on complex regulatory matters associated with data security, cyber incident response, the Committee on Foreign Investment in the United States and related export controls. He has assisted companies in most sectors of the economy on data security best practices and frequently assists with corporate due diligence. Mr Chipman currently serves as a non-resident fellow at the National Security Institute.

Benjamin Powell is a WilmerHale partner who has advised companies on major cybersecurity incidents and preparedness across virtually every sector, including banking, investment management, retail, defence and intelligence. He is recognised as a leading attorney in international investment and mergers, including the Committee on Foreign Investment and the Defense Security Service.

Arianna Evers is a WilmerHale special counsel who advises clients on complex privacy, data security and consumer protection issues. She helps clients with cybersecurity incident preparedness, incident response and internal investigations, and regulatory inquiries relating to data security breaches.

Shannon Togawa Mercer is a WilmerHale senior associate who advises clients on matters related to cybersecurity, privacy, and US and European data protection. She advises a broad range of clients in cybersecurity incident response and preparedness. She joined WilmerHale from the London location of a large global law firm where her practice focused on the cybersecurity and data protection aspects of capital markets transactions and mergers and acquisitions.

Cybersecurity continues to represent a growing risk for companies around the world with global cyberthreats posed by nation states, commercial competitors, company insiders, transnational organised crime and 'hacktivists'. The covid-19 pandemic made this trend particularly acute as businesses around the globe worked to navigate a more distributed workforce and more vectors for cyberattacks. The transition out of pandemic response has not brought with it any respite from these risks. Prominent ransomware attacks further substantiate concerns about destructive cybersecurity events that have an immediate impact on affected businesses. The ongoing conflict in Ukraine has also increased concern about cyber risk.

In this environment, maintaining an effective corporate cybersecurity programme is the standard expectation for all businesses and failure to do so increases risk for businesses as regulators and legislators remain actively engaged in this space. The ability to respond efficiently and effectively to data security emergencies will be important for avoiding potentially disruptive cybersecurity incidents in the future and for navigating related regulatory actions.

In the United States, while many standards promulgated in 2021 and 2022 related to federal agency security, proposed regulations in 2022 and 2023 reflect an ever-increasing focus on private sector cybersecurity, even in the context of the existing patchwork of state and federal regulatory guidelines and requirements. The current tenor of dialogue around cybersecurity regulation is unmistakeable – in its March 2023 National Cybersecurity Strategy the White House clearly states that 'Government's role is…to ensure private entities, particularly critical infrastructure, are protecting their systems.' The National Cybersecurity Strategy explicitly outlines the Biden administration's desire for legislation establishing liability for entities that 'introduce vulnerable products or services into our digital ecosystem' – in other words, manufacturers and software producers. The envisioned legislation will include a safe harbour framework

> "The Federal Trade Commission's enforcement actions continue to highlight its concern about company cybersecurity programs and data vulnerability on a technical level."

for companies that employ security best practices for software development.

In this environment, it is unsurprising that federal enforcement authorities are devoting growing resources to countering cyberthreats. For example, the Office of Financial Assets Controls (OFAC) issued an October 2020 directive, updated in September 2021, providing guidance specifically addressing ransomware events, warning potential victims that ransom payments could violate US sanctions laws. OFAC has also enforced sanctions against cryptocurrency exchanges that facilitate ransomware payments. The Securities and Exchange Commission (SEC) has been increasingly focused on expanding cybersecurity risk reporting requirements for public companies. The Federal Trade Commission's enforcement actions continue to highlight its concern about company cybersecurity programs and data vulnerability on a technical level. The Financial Industry Regulatory Authority and the SEC have also expressed additional focus on cyber-enabled fraud and identity theft prevention.

Federal data security regulatory requirements are most onerous for specific economic sectors believed to possess higher risk data, such as federal government defence contractors, financial institutions and healthcare companies. For example, on 15 March 2022, the Cyber Incident Reporting for Critical Infrastructure Act of 2022 was signed into law, creating new reporting requirements for critical infrastructure entities.

Previously, on 12 May 2021, President Joe Biden issued an executive order focused on combating threats to US computer systems. The Executive Order on Improving the Nation's Cybersecurity (Cybersecurity EO) set out to improve cybersecurity, particularly in relation to federal government systems, and followed several high-profile cyber incidents in 2020 and 2021. President Biden also issued an executive order mandating the US federal government to create new cybersecurity standards for all contractors. The Office

of Management and Budget (OMB) released software supply chain security guidance under the Cybersecurity EO directed at federal agencies and in May 2022, the National Institute of Standards and Technology (NIST) provided guidance on supply chain cyber risk for organisations.

There have also been numerous developments with respect to regulation of financial institutions. The Office of the Comptroller of the Currency, the Board of Governors of the Federal Reserve System, and the Federal Deposit Insurance Corporation issued a rule, effective on 1 April 2022, requiring banking organisations and service providers to report significant computer-security incidents to the regulators within 36 hours of discovery. In March 2023, the SEC separately proposed updates to Regulation S-P, which would, among other things, impose new cyber incident response and consumer data and information handling requirements on covered institutions.

While data security continues to be handled through sector-specific regulations and through state laws, there is an ongoing push for Congress to pass privacy legislation potentially similar in scope to the EU General Data Protection Regulation (GDPR). The proposed American Data Privacy and Protection Act bill is being revisited in 2023 by the House Committee on Energy and Commerce after a ground-breaking 2022 in which it became the first federal privacy bill to have made it out of committee. Many states in the United States are exploring the creation of new privacy rules that would include basic data safeguarding requirements, and California, Colorado, Virginia, Utah, Connecticut, Indiana, Tennessee, Texas, Montana and Iowa have all passed comprehensive laws requiring new privacy controls. State attorneys general continue to devote substantial resources to policing private sector data breach notification compliance. In addition; the New York Department of Financial Services, an institution known to be active in this space, has also proposed updates to its cybersecurity

Photo by Sean Pavone on Shutterstock

regulation, 23 NYCRR Part 500, would impose greater compliance requirements on covered entities.

Governments in Europe, Asia, South America, Central America and North America have been responding to the same trends, with particular focus on privacy and security controls for companies possessing large amounts of personal information.

In Europe, the regulatory environment remains fluid. Companies and regulators are still navigating the 2020 invalidation of the EU–US Privacy Shield framework, including uncertainty around the outcomes of related litigation, but there has been significant progress regarding a successor as the European Commission initiated the process to adopt an adequacy decision for the EU-US Data Privacy Framework (EU-US DPF) at the end of 2022. While the EU-US DPF continues to receive significant feedback from both sides, there remains a strong presumption that the requisite adequacy decision will be adopted in 2023.

"GDPR enforcement actions continue to grow. European regulators imposed over US$3 billion in fines in 2022 (as compared to around US$1 billion in 2021 and US$180 million in 2020)."

At the same time, companies in the European Union must continue to attend to cybersecurity and privacy compliance obligations under Directive (EU) 2022/2555 (or NIS2) that entered into force on 16 January 2023, the EU Cybersecurity Act (Regulation (EU) 2019/881) and existing and proposed requirements of the European Union Agency for Cybersecurity and the GDPR. The European Commission also proposed the draft Cyber Resilience Act in late 2022, focusing on the security of hardware and software development. GDPR enforcement actions continue to grow. European regulators imposed over US$3 billion in fines in 2022 (as compared to around US$1 billion in 2021 and US$180 million in 2020). Furthermore, after the UK formally left the EU (Brexit) in 2021 the UK Information Commissioner's Office has been active in staking out its own position on data protection, including through the introduction of UK-specific data transfer terms, and the Data Protection and Digital Information Bill on 8 March 2023, which provides some insight into potential reforms to the existing UK data protection regime.

In China, the Personal Information Protection Law (PIPL) has been in effect since 1 November 2021. Violations of the PIPL could lead to fines ranging between US$150,000 (or US$1,500 to US$15,000 fines on directly responsible supervisors or individuals) or in serious cases, US$7.7 million or up to 5 per cent of a company's previous year's business revenue. Furthermore, it is possible that for particularly serious instances of non-compliance, companies or their employees, or both, might be criminally liable. Notably, the PIPL applies not only to personal processing activities within China, but also to processing outside China of personal information of individuals who are inside China when the processing is for the purpose of providing products or services to individuals inside China, analysing or evaluating the behaviour of individuals inside China or for other circumstances prescribed by law or regulation.

The law includes parameters within which cross-border data transfers of personal information may be made for business and other reasons, including where consent or a security assessment may be required to effectuate the transfer. In February 2023, the Cyberspace Administration of China released the final version of the Measures on the Standard Contract for the Cross-Border Transfer of Personal Information (Measures) accompanied by the standard contractual clauses under the PIPL (Chinese SCC), effective on 1 June 2023.The Measures provide for a six-month period after 1 June until November 2023, for companies to comply.

Additionally, in December 2022, China published TC260-PG-20222A – The Practical Guide to Cybersecurity Standards – Specifications on Security Certification for Cross-Border Personal Information Processing Activities (V2.0-202212)), which are intended to implement the personal information (PI) protection certification regime as one of the three specified channels provided in article 38 of the PIPL.

Other Asian as well as African countries have also been actively legislating data protection and privacy, with Indonesia, Eswatini and Tanzania, all passing comprehensive laws in 2022, the Philippines, Singapore, Botswana and Uganda clarifying or amending established privacy laws, and Vietnam and Malaysia working through proposals. India's journey toward a comprehensive data protection law has been slow moving. In 2019, India introduced its Personal Data Protection Bill, on the heels of the 2018 EU General Data Protection Regulation. After years of deliberation, the bill was withdrawn on 3 August 2022. The Indian government has indicated that a new bill will be presented for public consultation.

In South America and Central America, Costa Rica, Panama and Uruguay made progress through proposed reforms and the adoption of additional measures in 2021. In 2022, Brazil continued its work implementing the Brazilian Data Protection Law (LGPD) and in February 2023, the Brazilian National Data Protection Authority (ANPD) adopted the Regulation on Setting and Application of Administrative Penalties under the LGPD, notably providing a framework for the administration of penalties and fines. With this regulation now in place, monetary penalties are anticipated. In March 2023, the ANPD published a list of entities (public and private) being investigated under the LGPD.

Data security requirements will continue to expand globally in the near term. For international companies, changing and expanding cybersecurity standards will continue to complicate company network security operations with special handling rules applying to the hosting and processing of sensitive data, such as personal data about consumers, critical infrastructure data and financial sector data. Cybersecurity will remain a major issue for these organisations and will continue to require technical, legal and communications experts to work together to manage the risk of data security incidents.

Jason Chipman
jason.chipman@wilmerhale.com

Benjamin Powell
benjamin.powell@wilmerhale.com

Arianna Evers
arianna.evers@wilmerhale.com

Shannon Togawa Mercer
shannon.mercer@wilmerhale.com

WilmerHale
Washington, DC
www.wilmerhale.com

Read more from this firm on Lexology

Photo by Weiming Xie on Shutterstock

China

Jingyuan Shi is the key contact for the Shenzhen office of Simmons & Simmons, and a partner leading the TMT practice in the Greater China region. She is a PRC-qualified lawyer and a practising solicitor in England and Wales.

Jingyuan specialises in data and technology laws. She has supported a large number of telecoms, media and technology (TMT) companies, strategic and financial investors in the TMT industry, asset managers, financial institutions, fintech companies and life science companies on an impressive selection of mandates, including without limitation data compliance, PE/VC and M&A transactions, regulatory and intellectual property.

Jingyuan is regularly invited to speak at industrial events. She is also a regular contributor to the Simmons & Simmons website and WeChat account, and for the China chapters of Lexology Getting The Deal Through: *Fintech* (2017–2023), *Telecoms & Media* (2017–2021), and *Market Intelligence*: *Privacy and Cybersecurity* (2021–2022).

Yuchen Lai is a legal executive in our Shenzhen office and a PRC qualified lawyer. She works extensively for international and Chinese telecoms, media and technology (TMT) companies, strategic and financial investors, financial institutions, asset managers, FinTech companies as well as life science companies. She advises on a wide range of compliance issues such as data and wider regulatory compliance, as well as corporate transactions. Yuchen has a strong focus on China data advice and has in-depth knowledge and rich experience in Chinese and global data compliance projects.

QUESTIONS

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

Over the past year, we have seen material regulatory updates in relation to cybersecurity matters in China, which, for the purpose of this chapter only, refers to mainland China, without taking into account the laws and practice in Hong Kong SAR, Macau SAR and the Taiwan region. The one with the widest influence is the implementation of two regulations in relation to cross-border data transfer (CBDT).

Restrictions on CBDT was introduced by China's Cybersecurity Law that took effect on 1 June 2017, which is the first legislation in China to comprehensively regulate the country's cyber networks. It applies to the construction, operation, maintenance and use of networks, as well as to cybersecurity supervision and management within the territory of China. Under the Cybersecurity Law, if an operator of 'critical information infrastructure' (CII) wishes to transfer personal information or 'important data' out of China, it must first clear the 'security assessment' (Security Assessment) organised by the Cyberspace Administration of China (CAC).

When the Personal Information Protection Law (PIPL), China's first comprehensive law on personal data protection, took effect on 1 November 2021, the Security Assessment requirement was extended to personal information processors (ie, equivalent to 'data controllers' under the General Data Protection regulation (GDPR)) that trigger certain data volume thresholds as determined by the CAC, though the PIPL itself does not clarify such thresholds.

However, the Security Assessment mechanism had not been officially implemented until 1 September 2022, when the Regulation on Security Assessment for Data Export (Security Assessment Regulation) was finally enacted, which clarifies that the following

situations will be subject to the Security Assessment requirement: (1) any data exporter to transfer 'important data' out of China; (2) any CII operator to transfer personal information out of China; (3) any personal information processor that processes the personal information of more than 1 million individuals to transfer personal information out of China; (4) any personal information processor that has transferred the personal information of 100,000 individuals or the sensitive personal information of 10,000 individuals out of China since 1 January of the previous year to transfer personal information out of China.

The Security Assessment is, in essence, a process of administrative approval. The substantial documents required for the process include an application form, a self-assessment report on data export risks and the legal document to be entered into by the data exporter and the overseas recipient. The data exporter needs to disclose to the CAC

detailed information about its business operations, data assets and processing activities, information systems and data centres involved in the intended CBDT, internal data security and privacy policies and procedures, as well as details of the overseas recipient. Further, the self-assessment report must also evaluate the data protection laws and practices in the destination jurisdiction, which is similar to the post-Schrems II 'transfer risk assessment' in the GDPR context.

Our observation is that in practice, the CAC applies very high standard when reviewing the application documents. According to official statements from provincial-level cyberspace administrations (PCAs), market players that have passed the Security Assessment by the end of May 2023 include Beijing Friendship Hospital, China Airline, Mazda, Sephora, HIK Vision and EZVIZ, etc.

The other important legislative update on CBDT is the Regulation on the Standard Contract for Personal Information Outbound Transfer (Standard Contract Regulation) as well as the annexed Standard Contract (China SCCs), which took effect as from 1 June 2023. Market players not subject to the Security Assessment obligation may use the China SCCs to transfer personal information out of China. The China SCCs share a fair amount of similarities with the EU's Standard Contractual Clauses for international data transfer (EU SCCs), whereas maintaining significant unique features, which international entities should note when implementing them and coordinating multi-jurisdictional data compliance.

For example, both the China SCCs and the EU SCCs are invariable fixed-form template contracts, the data exporter and the overseas recipient may only agree on limited additional clauses, which are not in conflict with the SCCs. Another example of the similarities is that both the EU SCCs and China SCCs are accompanied with the requirement of conducting impact or risk assessments on the proposed data transfers, which may be a challenging task to complete in practice.

Photo by Lili.Q on Shutterstock

As for the key divergences, the China SCCs in general do not differentiate different 'modules', except that a few clauses have set out different obligations for the overseas recipient, depending on whether it is a personal information processor or an entrusted party (ie equivalent to 'processor' under the GDPR). The Standard Contract Regulation also requires that the executed China SCCs along with the personal information protection impact assessment report shall be filed with the relevant PCA within 10 working days of the effective date of the executed China SCCs.

Another notable regulatory trend is that sectoral regulators in China are actively formulating or amending sector-specific rules in accordance with the principles under the Cybersecurity Law, the PIPL and the Data Security Law (effective as from 1 September 2021). To name a few, the new regulations issued over the past year include, among others, the Administrative Measures on the Cybersecurity of Medical Institutions, the Administrative Measures on the Cybersecurity of the Electricity Industry, the Administrative Measures on the Cyber and Information Security of the Securities and Futures

"In addition to mandatory regulations, over 20 recommendatory national standards in relation to cybersecurity were also published over the past year ."

Industry, and the Interim the Administrative Measures on Data Security in the Areas of Industry and Information Technology.

In addition to mandatory regulations, over 20 recommendatory national standards in relation to cybersecurity were also published over the past year. Though they are not legally binding, such standards may provide practical guidance for cybersecurity, data security and privacy practices relating to some specific sectors and application scenarios, including facial recognition, security protection of CII, instant messaging, e-commerce, online payment, cloud computing, edge computing, blockchain, notification and consent for personal information processing, etc.

Looking at the enforcement side, key regulators including the CAC, the Ministry of Public Security (MPS), the Ministry of Industry and Information Technology (MIIT), and the State Administration of Market Regulation (SAMR) continue to carry out regular enforcement against cybersecurity and privacy misconducts.

In July 2022, China's ride-hailing conglomerate Didi Global Inc (Didi) was fined 8.026 billion yuan by the CAC for violations of cybersecurity and data related laws. The cybersecurity review on Didi was initiated in July 2021. According to the official statement by the CAC, Didi's illegal conducts starting from June 2015 have 'imposed significant risks to the country's cybersecurity and data security', and 'seriously infringed the privacy and personal information rights of users'. The CAC also commented that Didi's violations involve an enormous amount of data (over 64.7 billion pieces), multiple types of sensitive personal information and various applications and processing activities, and the fine was based on the nature, duration and damage of Didi's illegal activities.

In March 2023, China's Cybersecurity Review Office (CRO) initiated an investigation on US semiconductor manufacturer Micron. The CRO stated in May 2023 that Micron did not pass the cybersecurity

review because it has 'severe cybersecurity problems' that could pose significant security risks to China's CII supply chain.

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?

The Cybersecurity Law requires network operators to notify competent regulators of cybersecurity incidents including personal information breaches, but it does not go on to provide details about the key factors to be assessed. A set of lower-level regulations and standards provide guidelines in this regard (including a new standard to take effect on 1 December 2023, of which the full text has not be published as of the date of this note). The reportable incidents usually include cyberattacks, hacking, malware, virus and human or equipment failure that may cause significant damage to the society and general public. Subject to the affected areas and degree of damage, there are different categories of reportable breaches. The key factors or impact of an incident that an organisation must assess include: (1) internet access in geographic areas (eg, single or multiple provinces, or even the entire country); (2) operation of major websites or platforms (eg, e-commerce websites with millions of active users); (3) number of users affected (a minimum of 100,000 users should ring alarm bells); (4) loss, theft or falsification of state secrets, important or core data that may cause significant damages; and (v) a catch-all scenario applicable to other factors, judged by the discretion of the organisation suffering the breach incident.

Upon initial assessment, if an organisation believes any of the above factors is met, it should immediately report such breaches to regulators. If a breach incident is likely to cause severe harm to the lawful rights and interests of individuals (eg, where sensitive personal information is leaked), the organisation shall inform the affected individuals of such breach incident.

Photo by Eric007 on Shutterstock

The PIPL requires the personal information processors (note the definition of personal information processor under Chinese law is essentially equivalent to the concept of a 'data controller' under the GDPR) to notify the competent regulator and relevant individuals once a personal data breach is detected. If the processor can take measures to effectively avoid the damage caused by data breaches, then it may decide not to notify the affected individuals. However, if the data protection regulators find the breaches may cause damage to individuals, they can request the processor to notify the affected individuals regardless. There is so far no general hard time requirement on when such report must be done under the PIPL, but we recommend data processors to report as soon as possible if initial assessments point to a report.

In addition, note that there are likely sectorial rules with more specific timing requests on this issue. For example, for financial

institutions, according to the Implementation Measures for Protecting Financial Consumers' Rights and Interests, which took effect on 1 November 2020, reports to consumers and the regulators must be made within 72 hours. The Measure for Supervising the Risks of Information Technology Outsourcing Activities by Banking and Insurance Institutions, which took effect on 30 December 2021, provides that banks shall report to China Banking and Insurance Regulatory Commission or its local counterparts within 24 hours of any client personal information breach or data damage/loss during the IT outsourcing activities. The Measures on Reporting, Investigation and Handling of Cybersecurity Incidents for Securities and Futures Sector, which took effect on 4 June 2021, provide that securities and futures institutions must report cybersecurity incidents immediately, and in the event of a severe incident the report shall be updated every 30 minutes. So, in addition to general reporting obligations, an organisation shall closely monitor and follow industry-specific regulations in order to comply with reporting obligations.

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

When hit with a data security incident, companies must be able to multitask on many pressing issues at the same time. The biggest issues include, but are not limited to, assessment of severity and scope of damage; determination of whether to report the incident to regulators and affected individuals; technical rectification measures to control the incident to minimise damage; complete and swift internal review and investigation of the breach; coordination with outside legal, forensic, technical or public relations counsel to prepare for subsequent actions; cooperation with directives from regulators and the police (if necessary); responses to customer inquiries or complaints; and responses to media reports or coverage.

"An organisation shall closely monitor and follow industry-specific regulations in order to comply with reporting obligations."

Any of these issues, if not handled properly, may easily morph into a situation that is out of control, especially in today's social media age. Such an incident is the true test of a company's response strategies, internal policies, management structure, designated staff as well as technical capabilities. The ultimate goal is to manage potential liabilities on all fronts, manage potential reputational damages, resume normal operation and prevent recurrence of similar incidents.

That said, out of these pressing issues, from a privacy protection perspective companies must concentrate resources to assess damages that may be caused to the privacy of affected individuals and take effective measures as a first priority to contain and control such damage while completing all legally required reporting and other obligations.

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

Following in the footsteps of the GDPR, China has made tremendous legislative efforts in data and cybersecurity related laws and regulations. Some high-profile pieces of legislation and investigation cases have conveyed strong messages to companies operating in China. We have seen many leading companies make good progress with regard to improving their cybersecurity preparedness.

First and foremost, the best practices are to comply with governing laws and regulations. Therefore, it is advisable to assess a company's actual compliance work against the laws and regulations and take measures to fix any gaps.

In addition to the mandatory laws and regulations, a company may need to comply with national and industry specific cybersecurity standards, including some technical standards as guidelines for their cybersecurity work. Typical examples include the Information Security Technology standards formulated by the National Information Security Standardization Technical Committee (almost all new standards mentioned in the previous sections fall within this series).

The Cybersecurity Law encourages companies to take security certifications. By going through the certification process, a company can evaluate its own practices against the certification standards and make changes accordingly to improve cybersecurity. Internationally recognised certifications, including without limitation ISO/IEC 27001, are being widely adopted by Chinese organisations as well.

As the regulatory framework in China on cybersecurity is still at a nascent stage, it is advisable to closely monitor the legislative process and implementations of the laws and regulations and potential impact over a company's business operations.

"By going through the certification process, a company can evaluate its own practices against the certification standards and make changes accordingly to improve cybersecurity. Internationally recognised certifications, including without limitation ISO/IEC 27001, are being widely adopted by Chinese organisations as well."

Photo by ESB Professional on Shutterstock

In terms of implementation of cybersecurity measures, companies need to mobilise resources to cover different areas. For example, they need to upgrade their IT infrastructure to maintain a high degree of cybersecurity; employ sufficient qualified technical staff; draft and implement necessary internal policies, especially an incident response policy; adjust the governance structure by appointing a data protection officer or similar roles; and seek readily available legal, forensic, technical and public relations advice in both the case of an incident and in their daily operation.

If any incident has escalated to a certain degree, companies tend to form special task forcse with in-house legal and technical staff and, if necessary, outside counsel as well, to address such incidents. It will help diffuse the situation in a professional and efficient way before it gets out of control.

QUESTIONS

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

Cloud services are one of the fastest growing areas in China in recent years. There are many factors for a company to consider and evaluate before it makes a decision to move data to a cloud hosting environment. These factors include, but are not limited to, security, flexibility, expansion capability, performance, cost, legal compliance, etc. If a company decides to go the cloud, the general recommendation is to assess the possibility of constructing the company's own private cloud system or to deploy hybrid cloud, and only if both are unrealistic, consider the public cloud.

With respect to special data security and privacy concerns, a company should evaluate such concerns in a larger context to determine the most suitable cloud service. As public cloud services cover a huge volume of users and multiple business models, they are more vulnerable to hacking. Hardware sharing is common for the public cloud. This means competitors using the same cloud services may share the same server. Further, the public cloud may not always meet certain compliance requirements, such as local storage of data. In contrast, a private cloud allows a company to deploy appropriate security measures as it sees fit, which will offer a higher degree of security. It is comparatively easier to meet compliance requirements using a private cloud. But the cost for a private cloud is also higher than the public cloud. Therefore, a company must strike a balance between the competing values of relevant factors in choosing cloud services. It is worth noting that two national standards related to cloud computing will take effect on 1 December 2023, which are the Security Guidance for Cloud Computing Services and the Security Capability Requirements for Cloud Computing Services, of which the full texts are not available as at the date of this chapter.

"Another notable concern is that cloud services are not entirely open for foreign investors in China. Foreign cloud service providers may need to cooperate with local partners to step into the China market."

In China, leading public cloud service providers include Alibaba, Tencent, Huawei, China Telecom and AWS. Although private cloud service providers, such as Huawei and Lenovo, are also available, the main users of private-only cloud services are comparatively limited to financial institutes in China. Companies with data security and privacy concerns tend to separate data into different categories based on the security grades. For example, a customer's credit card number will be stored on the private cloud with higher security protection. In contrast, official website content can be stored on the public cloud with less security protection. Such a hybrid cloud solution may also help the company to meet balace various compliance requirements with cost concerns.

A company shall closely monitor sector-specific regulations and standards with respect to cloud deployment. For example, the MIIT has published multiple recommendatory standards (non-binding) for the telecoms sector since mid-2021. The People's Bank of China has also published three recommendatory standards regarding cloud computing for financial institutions in late 2020.

Subject to its business model, a company shall closely monitor data security and privacy related laws and regulations. It shall design its core products or services from the beginning of its operation with a concept of categorised separation of data in accordance with applicable laws and regulations. This will prove more efficient and cost-effective for the company when it decides to go on the cloud later.

Further, cross-border transfer of data could be a key concern when considering cloud deployment. Pursuant to the relevant regulations, storing data overseas is deemed as a form of CBDT, hence companies will need to go through the Security Assessment or enter into the China SCCs with their cloud solution providers, if the cloud servers are located outside of China. In addition to generally appliable laws and regulations, companies in certain sectors (eg, financial

institutions, credit business agencies, insurance companies, medical institutions, ride-hailing service providers and smart cars) are also subject to sectoral data localisation requirements.

Another notable concern is that cloud services are not entirely open for foreign investors in China. Foreign cloud service providers may need to cooperate with local partners to step into the China market. Therefore, users of cloud service providers with a foreign background need to consider the business model of the service provider and consider whether it will have any impact on the services requested.

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

The Chinese government takes serious cybersecurity threats and criminal activity seriously.

The CAC is the main regulator with first-hand knowledge of market trends and cybersecurity threats through law enforcement activities, based on which it will lead the promulgation of new or amended regulations to address such concerns.

Owing to the rapid development of mobile technologies, CAC and other competent regulators such as the MIIT, the MPS and the SAMR have focused their law enforcement efforts in regulating mobile applications in recent years. These regulators have the authority under the law to request application stores to suspend or remove download channels for illegal applications. In the meantime, other sectoral regulators have also initiated special campaigns over the past year to urge relevant market players to identify and rectify non-compliant practices, such as the former China Banking and Insurance Regulatory Commission's campaign against banks and

Photo by askarim on Shutterstock

insurance companies, and the State Postal Administration's campaign targeting at delivery companies.

If any criminal offence leads are discovered during their investigation or review, such cases will be referred by the relevant regulators to the police to initiate criminal investigations. Individual citizens or entities, especially those victims of cybersecurity threats, are also encouraged to report crimes to the authorities, while providers of network products are legally obliged to report verified cybersecurity loopholes to the MIIT.

Law enforcement actions against cybersecurity threats are increasing. Civil lawsuits and public interest lawsuits against cybersecurity breaches are also increasing. According to statistics of the Supreme People's Procuratorate (SPP), over 6,000 public interest lawsuits for personal information protection were filed by procuratorates at various levels in 2022.

There are likely to be criminal liabilities for data violations. According to China's Criminal Law, criminal penalties for computer

"The SPC and provincial high courts regularly publish model cases in relation to cybersecurity crimes to raise public awareness and deter future offences. Although China does not have a case law tradition, to some degree these model cases also serve as precedents for lower-level courts to rule on cases."

hacking-related offences range from three- to five-year, or even longer, imprisonment sentences. For other crimes (eg, fraud, theft and embezzlement) conducted via cybersecurity breaches, penalties for the same crimes (conducted in a traditional offline matter as set out in the Criminal Law) will also apply. In addition, the Law on Anti-Telecom and Internet Fraud took effective on 1 December 2022. This new Law aims at preventing and combating relevant crimes by telecoms, finance and internet regulations.

The Supreme People's Court (SPC) and the SPP jointly issued the Judicial Interpretations on Several Issues Concerning the Application of Law in Handling Criminal Cases Involving Crimes of Illegally Using an Information Network or Providing Aid for Criminal Activities in Relation to the Information Network, which took effect on 1 November 2019. These judicial interpretations include quantified thresholds for punishable criminal offences, which provide guidelines to the police and prosecutors nationwide. The SPC and provincial high courts regularly publish model cases in relation to cybersecurity crimes to raise public awareness and deter future offences. Although China does not have a case law tradition, to some degree these model cases also serve as precedents for lower-level courts to rule on cases. As cybersecurity crimes tend to involve a large number of victims, the police and procuratorates usually take priority in handling these crimes.

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

The risk factors vary for different M&A deals. For asset or equity deals with high privacy and data security concerns (eg, purchase of software with heavy collection of user data or the equity of a hotel chain with large customer check-in data or equities of a manufacturer with a large number of employees worldwide, among many other examples)

privacy and data security liabilities should be a key, if not a deal-breaking, factor.

There are several steps to follow to minimise potential risks. First, a proper legal and technical due diligence must be done by the buyer. This is especially important for foreign investors who are not necessarily familiar with the relevant data implications in the China market. Often this exercise should be done against not only the Chinese law, but also the relevant laws to all the jurisdictions involved (eg, the portfolio companies have a cross-border structure established for capital financing reasons, or the investors have limited partners from different jurisdictions), which may trigger, among other things, cross-border data transfer concerns (again China has strict rules around cross-border data transfer). Note the due diligence findings may prove a no go, and if that is the case, of course, the earlier the finding is made, the better for both parties.

Second, subject to the due diligence findings, some rectification measures shall be taken either before signing, or as closing conditions or post-closing covenants (depending on circumstances). The buyer should consider requesting a reduction in the valuation of the target, escrow arrangement, etc, to hedge against potential liabilities. Certain representations and warranties should be customised with certain carve-outs to reflect the due diligence findings.

Third, subject to the magnitude of potential legal liabilities due to violations of privacy and data security, the buyer may insist on special compensation (which can be as severe as, for example, reversing the deal or down to the personal liabilities of the individual sellers) or offset of remaining payments (in the case of a payment schedule in several tranches with some payable after closing).

Fourth, the buyer should consider relevant insurance policies to cover liabilities for privacy and data security violations.

From the seller's perspective, it is important to shortlist credible buyer candidates. Once serious negotiations have commenced with selected buyers, the seller shall provide full disclosure to the buyers under a satisfactory confidentiality agreement. Properly documented full disclosure is the right defence for any subsequent buyer claim after closing. Further, as a general rule in M&A deals, the seller should consider setting certain time limits to provide any compensation, including for privacy and data security violations. Needless to say, operating in a compliant way (especially navigating the dynamic Chinese data law) from day one is important for the seller.

Jingyuan Shi
jingyuan.shi@simmons-simmons.com

Simmons & Simmons
Shenzhen
www.simmons-simmons.com

Yuchen Lai
yuchen.lai@simmons-simmons.com

Read more from this firm on Lexology

QUESTIONS

The Inside Track

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

Each law firm has its own focused practices. Clients should seek cybersecurity advice from lawyers who have a long-term track record of experience in navigating cybersecurity and data protection with a legal and a sectorial eye where relevant to the client. As cybersecurity often goes beyond national borders and, more importantly, nowadays data legislation from the key economies globally is influencing each other so heavily (especially the GDPR's impacts globally), lawyers with international practice and experience can offer more solid advice and input from a comparative perspective. Good lawyers are always on top of the latest legal developments. Last but not least, reputation or comments on lawyers generated from previous deals may also be key attributes clients should look for.

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

There are multiple layers of laws and regulations on cybersecurity and privacy in China. Some have only recently been adopted and without sufficient implementation rules, some may be in the draft stage, and the cybersecurity and privacy related legal framework is evolving at extremely fast pace, with new legislations or drafts coming out almost every month. We anticipate that this trend will continue in the next couple of years. In addition, multiple regulators may be in charge of the supervision of the same issues from different perspectives. Therefore, a client needs expert advice to help correctly analyse their case and navigate in the complex legal and regulatory framework for cybersecurity and privacy compliance in China.

How is the privacy landscape changing in your jurisdiction?

The triangulated safeguard for data regulation (ie, thee Cybersecurity Law, the Data Security Law and the PIPL) are all in place. Lower-level implementation regulations and recommendatory national standards are being drafted or amended accordingly. Key regulators will finalise their internal guidelines on law enforcement where applicable. Regional regulations on data and privacy are also emerging. All of these changes will shape the privacy and data protection regime in China. Businesses, especially multinational business undertakings with a China presence or selling products or services to China, would need to review their privacy approach to comply with these changes. Regulators are bringing enforcement up to speed with this new wave of legislation.

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

Business should be particularly aware of cybersecurity incidents that may cause massive data loss, paralyse internet access in wide geographic areas, affect a significant number of users, involve sensitive personal information, involve data (regardless of it being personal or non-personal data) in key sectors, stir up social unrest or involve state secrets, public interest or national security concerns.

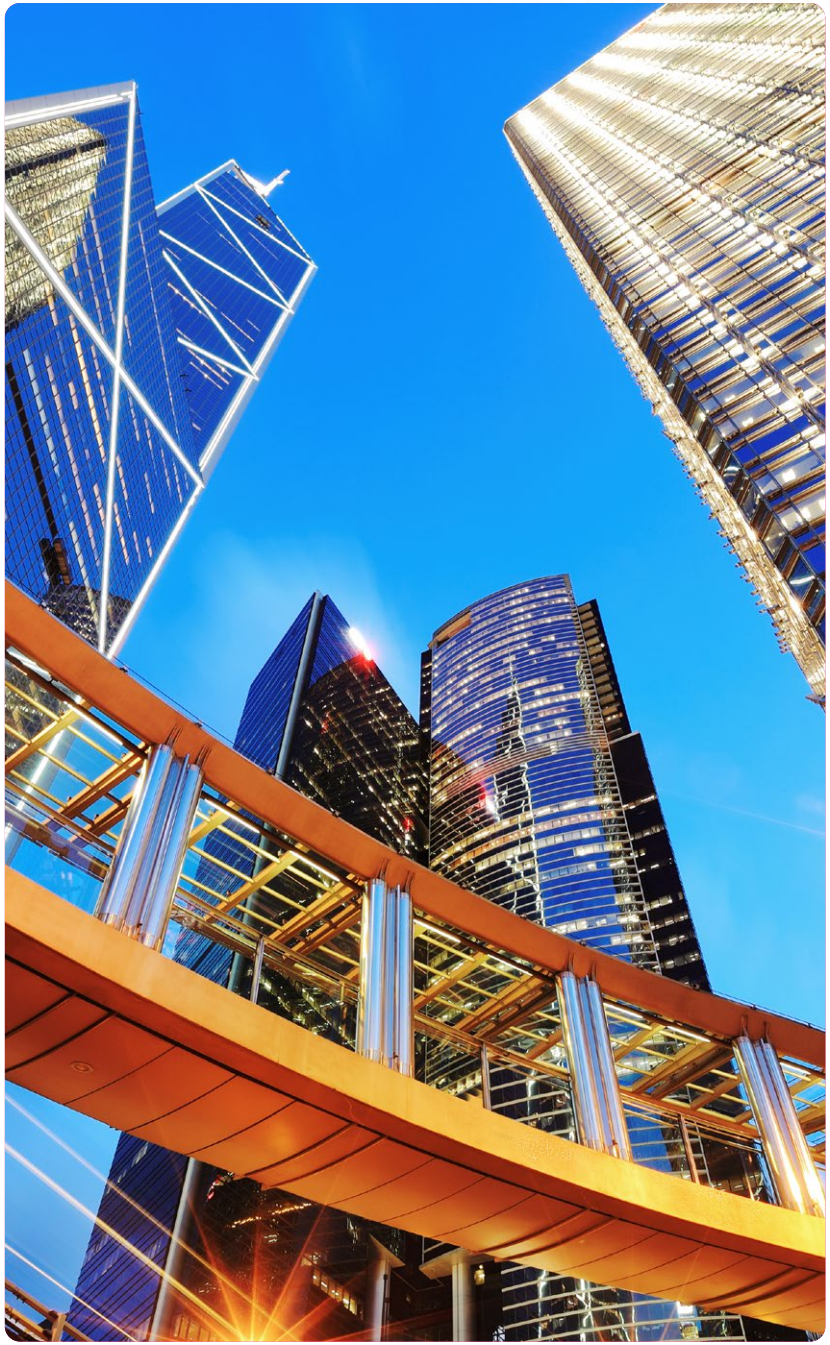


Photo by estherpoon on Shutterstock

Hong Kong

Michelle Ta at Simmons & Simmons has a breadth of experience across technology transactions, IT outsourcing, software and IP licensing, and privacy and data protection, and she has also made achievements in the field of financial technology. She has provided a series of data-related consulting services for virtual banks and fintech clients, and is currently seconded part-time to a virtual bank in Hong Kong to provide long-term legal support. Michelle is also an experienced cybersecurity legal adviser, and has acted in-house for a global IT services giant as the company's cybersecurity subject matter expert.

Clients have described Michelle as 'one of the few lawyers I would call having the full package', 'a lawyer to watch out for in the TMT sector' and having 'excellent technical skills and great commercial judgment across banking, technology and corporate practice'.

Michelle is dual-qualified in Hong Kong SAR and Victoria, Australia. She graduated from the University of Melbourne with first class honours in Law and holds a second bachelor degree in science, with double majors in biochemistry and biotechnology.

QUESTIONS

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

Hong Kong does not have a dedicated cybersecurity statute or mandated cybersecurity standards.

Instead, there are provisions governing cybersecurity and cybercrime in various pieces of legislation such as the Crimes Ordinance, the Telecommunications Ordinance, the Theft Ordinance, the Control of Obscene and Indecent Articles Ordinance and the Prevention of Child Pornography Ordinance.

The Hong Kong government announced plans to implement a new cybersecurity law to help ensure the security of Hong Kong's network information systems at a macro level in October 2021. In July 2022, the Cybercrime Sub-committee of the Law Reform Commission (LRC) published a consultation paper on Cyber-Dependent Crimes and Jurisdictional Issues, which sets out the preliminary proposals for law reform to address Hong Kong's challenges to cybercrime, uphold cybersecurity and safeguard national security. In considering these proposals, the LRC closely reviewed the cybersecurity standards adopted in other jurisdictions, including Australia, Canada, England and Wales, Mainland China, New Zealand, Singapore and the United States. The five cyber-dependent crimes (ie, crimes that can be committed only through the use of information and communications technology devices, where devices are both the tool and target of the crime) addressed include: (1) illegal access to program or data, (2) illegal interception of computer data, (3) illegal interference of computer data, (4) illegal interference of computer system, and (v) knowingly making available or possessing a device or data for the purpose of committing a crime. The LRC suggested that the borderless nature of cybercrime would justify the extra-territorial application of Hong Kong law and that Hong Kong courts should have


Michelle Ta

jurisdiction in cases where connections with Hong Kong exist (such as where the perpetrator's act has caused or may cause serious damage to Hong Kong). The LRC also recommended increased penalties and possible life imprisonment for aggravated offences (such as illegal interference with computer data or computer system).

As part of the consultation, the LRC sought responses mainly on the scope of exemptions and defences to the new proposed offences. The consultation period ended in October 2022 and the LRC has yet to publish the consultation conclusions as at May 2023. This is the first of three consultation papers to be published by the LRC. The second paper will focus on cyber-enabled crimes and the macro challenges in the digital age (including data sovereignty), whereas the third paper will address evidentiary and enforcement-related matters. We expect the remaining consultation papers to be published soon and further discussions to follow regarding the proposed regime.

"The Privacy Commissioner has also issued a number of new guidance notes to assist companies in uplifting their cybersecurity measures."

The Constitutional and Mainland Affairs Bureau of the Hong Kong Government's discussion paper on the review of the Personal Data (Privacy) Ordinance (PDPO), while issued some time ago in January 2020, remains noteworthy as it remains on the public radar for upcoming development in this space. The proposed amendments included are as follows:

- introducing a mandatory data breach notification requirement (as further discussed in question 2);
- introducing requirements to specify a retention period of personal data collected, which must be clearly communicated to data subjects via privacy policies;
- imposing stricter sanctions (such as pegging penalties to the data user's global annual turnover) and empowering the Privacy Commissioner for Personal Data (Privacy Commissioner) with the power to impose administrative fines directly in cases of breach;
- direct regulation of data processors (such as making data processors directly accountable for breaches);
- expanding the definition of 'personal data;' and
- implementing measures to combat doxxing.

Among the proposed amendments, as of May 2023, only anti-doxxing measures have been implemented, while the other proposed amendments to the PDPO are still under consideration.

There continues to be in place a variety of sector-specific requirements for regulated businesses, and cybersecurity continues to be an area of intense focus for financial regulators such as the Hong Kong Securities and Futures Commission (SFC) and Hong Kong Monetary Authority (HKMA). Recent efforts include the HKMA's upgraded Cybersecurity Fortification Initiative (CFI 2.0) and the SFC's thematic cybersecurity review of internet brokerages and further guidance on managing the cybersecurity risks of remote working, among others.

Albeit not legally binding, the Privacy Commissioner has also issued a number of new guidance notes to assist companies in uplifting their cybersecurity measures.

The Guidance on Recommended Model Contractual Clauses for Cross-border Transfer of Personal Data was issued May 2022, in which two new sets of recommended model contractual clauses (RMCs) were introduced, namely data-user-to-data user RMCs and data-user-to-data-processor RMCs. The data-user-to-data-user RMCs set out model clauses for data transfers between two data users (or data controllers) and are aimed at ensuring that a transferor takes all reasonable precautions to ensure that personal data transferred to a transferee acting in the capacity as a data user is not processed in a manner that would violate the PDPO. The data-user-to-data-processor RMCs sets out model clauses reflecting the PDPO

requirement that a data user remains accountable for the acts of its data processors and imposes contractual obligations to oblige data processor transferees to comply with the requirements of the PDPO. The RMCs are recommended by the Privacy Commissioner to be incorporated in agreements where personal data may be transferred outside of Hong Kong by a local entity to an overseas entity, or between two entities outside of Hong Kong where such transfer is controlled by a data user that is subject to the PDPO.

In reality, the RMCs are difficult to implement and are likely to be resisted by data processors, because they comprise certain obligations that lie beyond the control of data processors, such as requiring the transferee to ensure personal data transferred is adequate but not excessive. The actual law itself has not changed (and in particular, the relevant section of the PDPO (section 33) restricting cross-border transfer of data is still yet to come into effect). In February 2023, members of the Legislative Council expressed grave concerns about the slow progress of bringing section 33 of the PDPO into operation; however, no timetable has been announced for its implementation thus far.

Adoption of the RMCs is not mandatory. Organisations are also free to adapt and modify the RMCs or use alternative wording as long as they are consistent with PDPO requirements. As such, the RMCs are likely to be negotiated heavily by both data users and data processors, and we have not seen the same level of widespread use as that seen, for example, with the standard contractual clauses under the General Data Protection Regulation (GDPR) in Europe.

Another recent guidance from the Privacy Commissioner includes the Guidance Note on Data Security Measures for Information and Communications Technology issued in August 2022, which aims to provide data users with recommended data security measures for the ICT industry to facilitate their compliance with the relevant

Photo by estherpoon on Shutterstock

requirements under the PDPO and pointers towards good practices in strengthening their data security systems.

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?

There is currently no general mandatory data breach reporting regime in Hong Kong. Nonetheless, reporting of data breaches is encouraged by the Privacy Commissioner. In this regard, the Privacy Commissioner revised its Guidance on Data Breach Handling and the Giving of Breach Notifications (despite being non-legally binding guidelines) in January 2019, which provide data users with suggested practical steps to take in handling data breaches in order to mitigate the loss and damage caused to those involved.

"While we are yet to see legislative progress regarding a mandatory data breach notification regime, we expect this to stay high on the agenda in Hong Kong."

As a matter of practice, we see clients take a range of approaches to voluntary reporting (whether that is reporting to the regulator or affected consumers). Usually the factors that clients weigh up include whether the data breach might have to be reported on a mandatory basis in another jurisdiction (in which case, clients tend to lean to voluntary reporting in other affected jurisdictions); the size of the data breach; and the risk of harm to affected individuals. Factors such as negative public perception and financial consequences are also important considerations.

That said, since the start of 2020, the Hong Kong government has been discussing a range of changes to Hong Kong privacy laws, including introducing a mandatory data breach notification regime (as discussed in question 1). While we are yet to see legislative progress regarding a mandatory data breach notification regime, we expect this to stay high on the agenda in Hong Kong and that it may become law in the not-too-distant future.

Of course, for regulated businesses – and in particular, those subject to the supervision of financial regulators – there continue to be sector-specific regulatory expectations to report data incidents within certain time frames.

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

The biggest issues that companies need to consider from a privacy perspective arise even before companies suffer a data security incident.

First of all, data security (and privacy protection in particular) should be board-level issues. Too often, they are considered the sole domain of certain stakeholders (the Chief Information Security Officer, a data

protection officer or another 'tech' or 'legal' person) – so the first issue that companies need to address from a privacy perspective is an understanding that this is an enterprise-wide responsibility.

Dealing well with a data security incident starts from prevention in the first place, followed by good preparation for the worst-case scenario. The companies that do this best have a multidisciplinary team (stakeholders from senior management through to lawyers, public and government relations experts, cyber forensics professionals) that have been trained and drilled for cyber incident simulations so that they can mobilise quickly to respond to a data security incident when it (inevitably) occurs. Those companies know what steps they need to take and the order in which they need to take those steps – from initial containment of a data breach, through to ensuring key evidence is collected in a way that maintains chain-of-custody (particularly important so that digital evidence is not accidentally erased or changed in an effort to fix a breach), through to taking measures to fix vulnerabilities and post-mortem reviews. All of that will be important if a company is required to report an incident to a specific regulator (for example, the HKMA) or if the company decides it wants to voluntarily report the incident to the Privacy Commissioner or affected customers.

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

There are a range of approaches in Hong Kong to cybersecurity preparedness. Banks are among those that have the highest level of regulatory expectations when it comes to cybersecurity preparedness and cyber resilience. In terms of best practice, regulated banks in Hong Kong must meet a minimum baseline of cybersecurity readiness, which is set out in the HKMA's Cybersecurity Fortification Initiative. This comprises three pillars – (i) the Cyber Resilience

Photo by ESB Professional on Shutterstock

Assessment Framework, which helps banks assess their cyber risk posture and benchmark their level of defence and resilience; (ii) the Professional Development Programme, which is a certification scheme for cybersecurity practitioners in the industry to boost technical capability in areas such as attack simulation testing; and (iii) the Cyber Intelligence Sharing Platform, which is aimed at sharing cyberthreat intelligence to help the industry stay informed of, and prepare for, emerging hacking tactics and patterns.

This is consistent with common cybersecurity wisdom that cybersecurity is a patchwork of defences in an organisation's people, processes and technology.

Other sectors take a range of approaches to cybersecurity preparedness, and there remains a broad spectrum of cybersecurity maturity levels in Hong Kong.

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

Yes – in particular organisations that are supervised by the SFC and HKMA in Hong Kong should in particular be aware of the requirements and best practice imposed by each of these regulators.

For licensed corporations regulated by the SFC, additional requirements are imposed by the SFC on the use of external electronic data storage services (like cloud hosting services) to store their data and records. The SFC issued a Circular in late 2019, and in late 2020 a set of accompanying FAQs, setting out certain requirements for licensed corporations wishing to move their data storage to a cloud hosted environment. Some of the requirements set out in this regime impose expectations that are rather unusual both from the perspective of cloud service agreements in a broader sector-agnostic context as well as when contrasted with expectations in similar sectors of other jurisdictions. This includes, for example, a requirement to maintain a full and immutable audit trail to memorialise access logs by every unique user of a data record.

Authorised institutions regulated by the HKMA should be aware of the Guidance on Cloud Computing issued by the HKMA in August 2022, which addresses the increased cyber risks that come into play as authorised institutions begin to deploy cloud services for more important functions (and not merely for basic and non-core operations only) over recent years. Authorised institutions are recommended to put in place an effective governance framework and carry out proper due diligence of the cloud service provider. Ongoing risk management and controls are recommended for the authorised institution to continually monitor and mitigate risks as necessary. Authorised institutions should also ensure that suitable arrangements are made

"Some of the requirements set out in this regime impose expectations that are rather unusual both from the perspective of cloud service agreements in a broader sector-agnostic context as well as when contrasted with expectations in similar sectors of other jurisdictions."

to allow it to comply with HKMA's supervisory access and other supervisory expectations. Topping that off, authorised institutions should equip staff overseeing cloud operations with adequate knowledge and skills to securely use and manage the risks associated with cloud computing.

Outside these requirements of the SFC and the HKMA, there are of course all the usual requirements that businesses (both regulated and non-regulated) should generally consider when thinking about moving data to an environment hosted by a third party – including due diligence to ensure that the relevant cloud product is fit for the intended purpose, that the vendor is certified against prevailing industry cybersecurity standards, that the vendor can meet required data availability and uptime commitments and that there is a certain level of redundancy and disaster recovery to guard against data loss.

In addition, cross-border data transfer restrictions and increased exposure to mandatory government or regulatory access to cloud hosted data (and in some cases, conflict of law issues) remain important considerations when looking to move data to the cloud.

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

A specialist unit within the Hong Kong Police – the Cyber Security and Technology Crime Bureau – is responsible for investigating and handling technology crime, computer examinations and preventing technology crime.

In addition, as discussed in further detail above in question 1, an amendment was passed in 2021 to reform the PDPO to combat malicious doxxing acts and protect the public's personal privacy. A raft of new enforcement powers were also conferred on the Privacy

Photo by I and S Walker on Shutterstock

Commissioner to investigate and prosecute doxxing crimes, as well as granting the Privacy Commissioner with the power to issue cessation notices with extraterritorial effect.

In relation to the proposed development of a local cybersecurity law, the LRC's consultation paper on Cyber-Dependent Crimes and Jurisdictional Issues in July 2022 (as discussed in question 1) is the first of three consultation papers to introduce proposed legal reforms (of which the third paper is expected to cover enforcement-related issues). We expect to see further efforts in enhancing the cybersecurity of critical infrastructure in Hong Kong through legislation that will seek to require all private and public enterprises to comply with cybersecurity regulations.

QUESTIONS

> “ A history of multiple or serious non-compliances with applicable data law spotted during the due diligence process may affect the value, terms or indeed continuation of the deal.”

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

All companies should be doing appropriate level of privacy and data security due diligence when looking at a potential acquisition or merger target. This involves due diligence from a legal perspective (eg, whether there have been any recent mandatory or voluntary data breaches notified to regulators, whether there have been any near misses and whether there have been any data handling complaints or litigation that may indicate a systemic issue), as well as from a technical perspective (eg, bringing in cybersecurity professionals to assess a potential target's cybersecurity posture). This is particularly important for companies that engage in businesses that are data-intensive, businesses that interface directly with consumers or businesses that are subject to particularly strict privacy laws in other jurisdictions. A history of multiple or serious non-compliances with applicable data law spotted during the due diligence process may affect the value, terms or indeed continuation of the deal. These risks should also factor into decisions about M&A deal shapes and ways in which sellers may be required to remain financially responsible or accept more onerous terms for latent privacy and data security issues.

Michelle Ta
michelle.ta@simmons-simmons.com

Simmons & Simmons
Hong Kong
www.simmons-simmons.com

Read more from this firm on Lexology

QUESTIONS

The Inside Track

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

Clients should look for curious lawyers with an in-depth understanding of technology, computers and cybersecurity as a discipline (ie, knowledge beyond the strictly legal) with a good team of litigator colleagues working alongside them to cover tricky dealings with customers or regulators. It is important to look for a team with a good working knowledge of data law across multiple jurisdictions.

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

The fact that Hong Kong data law has been around for so long (since 1995!) and remains relatively unchanged today is a very interesting contrast to the pace of change in data regulation in other parts of the world – this is particularly the case as many multinational companies have their Asia headquarters in Hong Kong, and the interplay in practice between different laws can become very complex and interesting as data itself often lives in more than one location in today's cloud-reliant business environment.

How is the privacy landscape changing in your jurisdiction?

Hong Kong's data and privacy laws definitely win the prize for longevity! They are due for a change (although I am constantly amazed at the resilience of the PDPO and how well a law drafted in 1995 still holds up and adapts so well to so many novel practical situations today).

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

In Hong Kong, phishing still remains one of the top tactics for bad actors to infiltrate systems. Threat actors are becoming more sophisticated and more patient and will wait longer to execute large-scale attacks, such as targeted emails to senior executives to trick them into transferring large sums of their business.

Photo by MORENO01 on Shutterstock

Italy

Paolo Balboni is a founding partner of ICT Legal Consulting and professor of privacy, cybersecurity and IT contract law at the European Centre on Privacy and Cybersecurity Faculty of Law Maastricht University. He advises clients on legal issues related to cybersecurity, privacy and data protection, IT contracts, cloud/edge/quantum computing, artificial intelligence (AI), big data and smart analytics and the internet of things, among others.

Luca Bolognini is a founding partner of ICT Legal Consulting and president of the Italian Institute for Privacy and Data Enhancement. Attorney-at-law, DPO and ethics and privacy adviser in EU projects. Luca serves as an independent Ethics and Privacy Advisor for several European research and innovation projects (Horizon 2020/ Horizon Europe).

Floriana Francesconi is a lawyer and arbitrator registered with the Bologna Bar Association. She is an expert in labour law and a TÜV Italy certified privacy consultant.

Francesca Tugnoli is a lawyer specialising in corporate criminal law, privacy and 231. Research doctor in criminal law, specialising cum laude at the E Redenti school, graduated maxima cum laude in law.

Francesco Capparelli is an attorney at law, a Certified Ethical Hacker, with a master's degree in cybersecurity and in competition and innovation law (big data and privacy).

Andrea Sudano graduated in law at the University of Milan. He has a master's in cybersecurity and defence at the University of Catania.

QUESTIONS

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

In the past few years, we have borne witness to the evolution of an exceptionally innovative legal framework, designed to safeguard the functions of state entities. A pioneering instance of this at the European level is Directive (EU) 2016/1148 of 6 July 2016, concerning measures for a high common level of security of network and information systems across the Union (commonly known as the NIS Directive). This directive was incorporated into Italian legislation through Legislative Decree No. 65 of 18 May 2018.

Building upon this, Decree-Law No. 105 of 2019 (later converted and amended by Law No. 133 of 18 November 2019) formally instituted the National Cybersecurity Perimeter (PNSC). This perimeter serves to ensure a high level of security for networks, information systems, and digital services related to both the public administration and national, public, and private entities and operators.

In alignment with Decree-Law No. 105, Prime Ministerial Decree No. 131 of 30 July 2020 laid out the criteria for identifying the entities included within the PNSC and the associated obligations from a national security protection perspective. These entities span a range of sectors, such as space and aerospace, energy, telecommunications, transport, digital services, and health and social security institutions. They are obligated to identify in advance the Information and Communication Technology (ICT) assets deemed critical for executing the activities outlined above, with the objective of ensuring the integrity, efficiency and security of data and all processed information.

Entities included in the Perimeter are expected to undertake a range of activities, including the annual updating of their ICT asset lists, conducting risk assessments to identify potential risk factors, and the establishment and execution of necessary security measures.


Paolo Balboni


Luca Bolognini


Floriana Francesconi

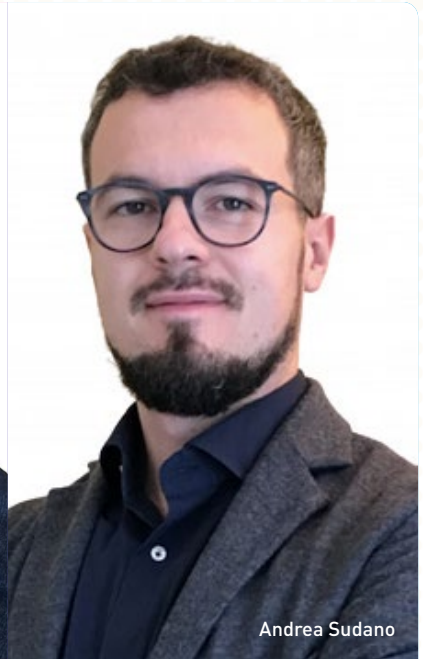

Francesca Tugnoli

Building upon this, the Directorial Decree of January 2023, issued by the National Cybersecurity Agency, stated that from 2024 onward, any company seeking to work with the Italian public administration must obtain certification relative to the type of information it processes. Specifically, if a company processes strategic information related to the Italian Public Administration, it must hold certifications for ISO 9001, ISO 27001, ISO 20000-1 and ISO 22301. This requirement underscores the escalating importance of robust cybersecurity measures and compliance in protecting national interests and maintaining the integrity of public administration activities.

Significantly, at the end of 2022, the NIS Directive was superseded by the NIS 2 Directive, marking a new era in European cybersecurity regulation. Member states have been given over a year to 'transpose the obligations of the directive' into their national legislation, reflecting the need to continually adapt and evolve to meet the increasingly sophisticated and complex cybersecurity challenges.

The evolution of cybersecurity requirements and the increasing emphasis on data protection have also ushered in an important update to the ISO 27001 standard. The ISO 27001:2013 version has been superseded by ISO 27001:2022, reflecting advancements in information security management practices and the need to address new cybersecurity threats. This updated standard reinforces the importance of establishing, implementing, maintaining and continually improving an information security management system within the context of the organisation. It also underlines the necessity of assessing and treating information security risks tailored to the needs of individual organisations. As such, organisations seeking to work with the Italian public administration will need to ensure that their information security practices align with the requirements of ISO 27001:2022, further demonstrating the ongoing importance of robust, up-to-date cybersecurity measures in today's digital landscape.


Francesco Capparelli


Andrea Sudano

Last but not least, the Digital Operational Resilience Act (DORA) regulation forms part of a broader European package of strategic measures for both traditional and fintech sectors. The primary objective is to ensure that businesses in these sectors are capable of combating cyberattacks through the implementation of measures concerning governance, cybersecurity, ICT risk management and incident reporting.

DORA aims to create a Risk Management Framework to ensure the digital resilience of financial organisations. It outlines six distinct 'pillars' that organisations must implement.

ICT Governance is aimed at encouraging a better alignment of ICT risk management strategies within financial institutions. The role of management is vital in allocating responsibilities and roles for all ICT

QUESTIONS

functions, monitoring ICT risk management and ensuring appropriate investment and training in ICT.

ICT Risk Management seeks to enhance and harmonise the rules for managing ICT risk. Financial entities are tasked with creating and maintaining resilient ICT systems through the identification of ICT risks, developing protective and preventive measures, detecting threats, managing incidents and implementing strategies for operational continuity and disaster recovery.

Incident Management introduces specific obligations related to the management of ICT incidents. Organisations are required to implement a system that classifies various incidents based on criteria outlined in the regulation and further defined by European supervisory authorities to establish relevance thresholds.

Resilience Testing is a significant addition, specifying that financial entities must regularly undergo testing to assess their maturity level, identify weaknesses and establish any necessary corrective measures. This pillar emphasises the regulator's aim to adopt a proactive approach that surpasses simple reactive corrective measures. Only authorised and suitably certified entities can carry out activities such as Penetration Testing and Red Teaming.

Third-Party Risks stipulates that entities must ensure adherence to rules concerning the monitoring of ICT risks associated with third parties. It also calls for the harmonisation of essential service elements throughout all stages of the contract: initiation, execution, termination and post-contract phase.

Information Sharing is designed to address the communication gap among various entities within the European Community. It allows financial organisations to agree to share information and data on cyber threats, thereby bolstering cooperation among member states.

Photo by imageBROKER.com on Shutterstock

QUESTIONS

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?

In the landscape of cybersecurity, a security breach has the potential to inflict significant damage through the destruction, loss, modification, or unauthorised disclosure of, or access to, personal data in transmission, storage or undergoing processing. These breaches may manifest as illicit acts or unintentional accidents, threatening the confidentiality, integrity and availability of personal data.

To illustrate, one can consider the incidence of access to personal data in events such as unauthorised acquisition of data by third parties, theft or loss of computing devices harbouring personal data, accidental loss or destruction of personal data, and unsanctioned

> "Data controllers or processors are mandated to document all breaches in a comprehensive register."

disclosure of personal data. Any or all of these events may coexist and accumulate, amplifying the risk to data security.

The data controller, irrespective of whether it is a public entity, private company, association or another organisation, has a mandate to report any breach to the Italian Data Protection Authority. This action should be undertaken promptly, ideally within 72 hours of becoming aware of the breach. Similarly, data processors cognisant of a potential breach must alert the data controller without delay, allowing for the initiation of remedial measures. Any notification submitted to the Italian Data Protection Authority beyond the stipulated 72-hour window should be supplemented with a justification for the tardiness.

Furthermore, if a personal data breach harbours a high risk to the rights and liberties of individuals, the concerned individuals must be notified. Notwithstanding the notification to the Italian Data Protection Authority, data controllers or processors are mandated to document all breaches in a comprehensive register. This serves as a record for potential verification activities undertaken by the Authority in compliance with regulatory frameworks.

However, in terms of impact analysis, the severity of a data violation is intrinsically tied to the nature of the breached data. Breaches involving sensitive data, such as financial details or data relating to health, religious or political orientations, invariably imply heightened risk to the concerned individuals. Conversely, breaches confined to general information, such as names or email addresses, may pose a relatively lower risk.

From an evaluative standpoint, it is crucial to ascertain if the breach could result in physical, material or immaterial harm to individuals. The occurrence of a personal data breach, particularly involving sensitive data, may yield discriminatory, reputational or financial impacts. Therefore, each breach must be evaluated on an incident-specific basis, as seemingly similar breaches can have vastly different consequences.

In this context, the Recommendations proposed by the European Union Agency for Cybersecurity provide an invaluable framework for assessing personal data breaches. Moreover, the Guidelines issued by the European Data Protection Board (EDPB) serve as a compendium of historical notifications and a valuable resource for data controllers throughout the incident management lifecycle – from initial risk and threat assessment, to evaluation of preventive measures and, finally, to incident resolution.

Under the DORA, organisations are required to establish a comprehensive incident management program to effectively identify, manage and report ICT incidents.

DORA mandates a comprehensive approach to handling ICT incidents. Organisations are required to establish a systematic method for mapping and categorising such incidents based on predefined criteria, helping determine their severity and appropriate response actions.

QUESTIONS

This incident mapping is coupled with a requirement for prompt reporting of significant events to the relevant supervisory authority, which facilitates monitoring of systemic risk, trend identification and the development of preventative measures.

Furthermore, DORA stipulates that organisations must have clear incident management processes, including predefined roles and responsibilities, as well as mechanisms for incident detection, assessment, containment, eradication and recovery. This aligns with the requirement for operational continuity and disaster recovery planning, ensuring that organisations can maintain or swiftly resume operations post-incident and recover from potential disaster scenarios.

Finally, to guarantee the resilience of ICT systems, organisations are mandated to periodically conduct resilience testing. These tests aim to identify vulnerabilities, assess the system's maturity level, and outline any necessary corrective measures, thereby ensuring that systems can withstand and recover from unexpected disruptions.

Overall, the incident obligations under DORA emphasise a proactive and comprehensive approach to ICT risk management, designed to improve the digital resilience of organisations in the financial sector.

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

The ramifications stemming from a cybersecurity incident are multifaceted and hinge upon the nature of the organisation affected, the data compromised, and the incident management proficiency exhibited. To buffer against the potential impacts of such incidents, it is of paramount importance to arm the organisation with both technical and organisational measures calibrated to mitigate the incident.

Photo by Boris Stroujko on Shutterstock

From an organisational viewpoint, drafting, documenting, and periodically updating an IT security incident response plan is a strategic imperative. This plan should encompass the mobilisation of pertinent functions for optimal and efficient incident management. By doing so, the organisation is better positioned to mitigate associated risks and minimise the impact of the incident. Furthermore, the presence of a robust incident management plan bolsters the organisation's resilience, allowing for the continuity of its critical operations, thus safeguarding its reputation.

From a technical standpoint, the organisation must adopt incident detection solutions, such as a security information and event management system or a security operations centre (SOC). The former is a system that aggregates logs and events generated by networked applications and systems, enabling security analysts to expedite the resolution and investigation of security alerts and

"Many organisations opt to notify data subjects of a breach, even when not mandated by the GDPR, as a demonstration of their commitment to data security. This proactive approach fosters a relationship of trust with their customers."

incidents. The latter, SOC, serves as a hub where information concerning the security status of an organisation's IT environment (or multiple organisations' environments in the case of a managed security service provider is centralised.

Additionally, it is critical to establish clear roles, responsibilities, and timelines for each manager and formalise these in a comprehensive procedure. The incident response team also assumes a pivotal role. Their initial task is to evaluate the incident and determine whether it constitutes a data breach. If the incident indeed involves a data breach, the organisation must assess, under article 33 of the General Data Protection Regulation (GDPR), whether the incident warrants notification to the Authority and the data subjects impacted by the breach. To optimally execute this task, we recommend that the organisation establish both a data breach assessment unit and a data breach management unit. It should be noted that the risk could be made public even if there is no obligation to notify data subjects, such as in the case of a phishing attack. This could potentially trigger an economic impact – due to fines imposed on the organisation – and a reputational fallout that may result in contractual losses with partners and suppliers.

Given these considerations, we counsel our clients to adopt a proactive stance towards data breach communication. Many organisations opt to notify data subjects of a breach, even when not mandated by the GDPR, as a demonstration of their commitment to data security. This proactive approach fosters a relationship of trust with their customers. It is crucial that organisations not only acknowledge the impact of a data breach but also strive to be perceived as trustworthy by implementing appropriate technical and organisational measures. This includes providing staff training to reduce the risk of human error. Finally, in instances where the incident is a result of a deliberate act, we advise reporting the incident

to law enforcement agencies to preclude potential allegations of complicity or collusion with the attackers.

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

A paramount security measure adopted by organisations is the orchestration of comprehensive training programs for personnel. This dual-pronged approach focuses on enhancing the competency and awareness of employees, while simultaneously mitigating human error – a risk factor that poses significant threats to organisations absent ongoing training initiatives. Consequently, training should encapsulate both the primary cybersecurity threats and the behavioural protocols necessary to curtail such threats.

In this digital era, online platforms serve as an optimal conduit for executing targeted courses, such as webinars, training events and competency tests. These platforms facilitate the augmentation of staff awareness, presenting theoretical cybersecurity concepts and practical activities, such as post-training assessments, to reinforce learning outcomes regarding cybersecurity and privacy issues.

In addition to training, formalising best practices in accordance with leading international standards for privacy and cybersecurity is a critical security measure. This is manifested through the formulation of robust policies and procedures that resonate with the organisation's cybersecurity posture.

Lastly, executing comprehensive controls on human resources serves as a potent security measure, aimed at attenuating the probability of accidental or malicious threats. For instance, conducting background checks and assessing the competencies of all prospective employees

Photo by VILTVART on Shutterstock

can significantly decrease the likelihood of internal threats, thus bolstering the organisation's overall cybersecurity framework.

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

As the utilisation of cloud technology for data storage proliferates, the focus on securing the data within these systems intensifies, particularly when these clouds harbour personal data. This context brings two international standards to the fore, namely ISO 27017 and ISO 27018. These standards augment the controls of ISO/IEC 27001, introducing additional, specific controls.

ISO 27017, titled 'Code of Practice for Information Security Controls Based on ISO/IEC 27002 for Cloud Services', delineates general security controls for cloud service providers and their clientele. Conversely, ISO 27018, titled 'Code of Conduct for the Protection of

QUESTIONS

"The EU Cloud Code and the Cloud Infrastructure Service Providers Code, both endorsed by the EDPB, serve as critical references for personal data protection and cloud computing."

Personally Identifiable Information (PII) in Public Clouds Acting as PII Managers', serves as a code of conduct for cloud providers, placing emphasis on protecting PII within public cloud services. The latter offers guidelines for cloud providers functioning as data controllers. These standards should be embedded within ISO 27001 certification when the scope encompasses cloud services, necessitating specific training on cloud technology, particularly its critical elements and access rights management. This training should cater to administrators, users, employees and third parties.

When transitioning to a cloud-hosting environment, business continuity is critical, as mandated by ISO 22301 'Societal security – Business Continuity Management Systems – Requirement'. This standard pertains to the construction and continual enhancement of business resilience, outlining the requirements necessary for planning, implementing and monitoring a documented management system focused on continuous improvement. Compliance ensures increased protection of organisational information, reducing the incidence of business or security incidents, and optimising response and recovery times after a security incident.

The ANSI/TIA-942 standard for data centre protection is also noteworthy. The American National Standards Institute (ANSI) validates guidelines for infrastructure construction, while the Telecommunications Industry Association is an ANSI-accredited body, voluntarily developing consensus-based standards for diverse ICT products.

Additionally, the EU Cloud Code and the Cloud Infrastructure Service Providers Code, both endorsed by the EDPB, serve as critical references for personal data protection and cloud computing.

Consequently, organisations should conduct comprehensive assessments of cloud solution providers, scrutinising their technical and organisational security measures, with keen attention to data

centre locations. This is paramount given the global dispersion of data centres utilised by many cloud providers, some of which are located outside the European Economic Area. As per article 46 of the GDPR, appropriate safeguard clauses are provided for such trans-border transfers aimed at data protection. Moreover, companies relying on cloud providers must ensure the legitimacy of data transfers, considering the requirements set forth by the European Court of Justice – in light of the *Schrems II* judgment – and the recommendations proposed by the EDPB.

Lastly, the client using the cloud service provider must evaluate the risks associated with data transfers, determining the likelihood and potential impacts. This necessitates analysing the security measures implemented by the provider to minimise impacts, as well as any additional security measures required to mitigate potential impacts. According to the EDPB recommendations and the *Schrems II* judgment, if the anticipated security measures are not fully adopted, rendering them insufficient, the transfer should be suspended or the relevant supervisory authority notified.

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

The Italian government has instituted a dedicated national police unit designe to investigate cybercrimes and cyberterrorism, and to safeguard critical national infrastructure. Moreover, through Legislative Decree 65/2018, the Italian Computer Security Incident Response Team (CSIRT) was formed, housed within the Department for Information Security of the Presidency of the Council of Ministers. The CSIRT's primary role is to supervise incidents at a national level, playing a crucial role within a network of CSIRTs appointed by EU member states.

Photo by Stefano Panzeri on Shutterstock

The CSIRT's responsibilities extend to issuing early warnings, alerts, and announcements. They also include disseminating relevant information concerning risks and incidents to pertinent parties, and most critically, intervening in cases of cybersecurity incidents. These measures are integral to the proactive management of potential cyber threats and the effective containment and resolution of incidents when they occur.

Within the context of Italian criminal law, myriad computer-related offenses are punished under the Penal Code. Examples of these offenses include unauthorised access to computer systems, damage to computer systems, and computer fraud, respectively outlined in articles 615-ter, 635-bis, 635-quater and 640-ter of the Penal Code. These provisions encompass a broad range of actions that can be perpetrated using digital tools. The penalties for these crimes are particularly severe if committed by individuals in roles such as system administrators, and they become prosecutable ex officio.

QUESTIONS

"It is crucial to emphasise that adherence to data privacy regulations and meticulous protection of data, including its quality, are vital parameters in assessing the actual value of the databases and information resources of the target organisation."

In a recent ruling, the Italian Supreme Court interpreted digital documents as assets whose content is susceptible to theft, thus qualifying for the penalisation of theft under article 624 of the Penal Code. In the context of the Italian criminal legislative landscape, the aforementioned computer crimes are also significant in relation to Legislative Decree 231/2001, article 24-bis. This provision implies that if such crimes are committed in the interest of a legal entity, the corporate body could be held accountable for these offences.

Furthermore, under the regulations established through Law 105/2019, which outlines the boundaries of the National Cyber Security Perimeter, there is a legal obligation for organisations to report cybersecurity incidents. This obligation emphasises the importance of transparency in the face of potential threats and serves to ensure that appropriate measures can be taken swiftly to address and mitigate the impacts of such incidents. It underscores the overall significance of an effective cybersecurity strategy in maintaining the integrity and security of digital assets and infrastructure at the national level.

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

In the intricate process of M&A, one paramount element to consider is the information technology (IT) risk level of the target organisation, including the security measures it has established to safeguard its information assets. This necessitates a comprehensive examination of data protection compliance and cybersecurity due diligence.

It is crucial to emphasise that adherence to data privacy regulations and meticulous protection of data, including its quality, are vital parameters in assessing the actual value of the databases and

information resources of the target organisation. For instance, a substantial database of clients or prospective clients can significantly influence negotiations. However, if this database has been established without full compliance to privacy laws, such as if proper consent has not been obtained from the data subjects, the risk is considerable, potentially rendering the entire dataset unusable and necessitating deletion.

Simultaneously, an objective, security risk-based approach should be employed to ascertain and evaluate potential cybersecurity threats that could affect the target organisation, taking into account the probability of their occurrence and potential impact. An initial assessment should be performed, encompassing all aspects with significant influence on the business and potential threats that could impact stakeholders during and post-M&A process.

A thorough evaluation of the target organisation's cyber governance is essential, considering the technical and organisational measures implemented, resources utilised and the level of corporate awareness. It is crucial to verify regular privacy and cybersecurity training within the target organisation, and the implementation of internal security measures intended to certify the effectiveness and efficiency of all cybersecurity-related activities. These activities may include software and firmware updates, review of authorisation profiles, firewall rules and other configurations, resource inventory management, prevention and detection of potential attacks from both external and internal sources, and incident response and recovery management.

Quantifying the value of all the target organisation's information assets, particularly if these are integral to the core business, is also significant for assessing the potential impact of security incidents. The impact can often depend on the types of technology platforms utilised by the target organisation (eg, cloud-based, on-premises, physical or virtual machines, choice of operating systems and databases) and the consequent security measures implemented.

Furthermore, vulnerability assessment and penetration testing are critical components in this evaluation process. These activities help in identifying potential vulnerabilities in the target organisation's systems and evaluating how resilient the systems are to cyber-attacks.

Lastly, if the target organisation utilises third-party vendors, it is advisable to assess the security measures those vendors have implemented both within their organisation and in relation to the service or product offered to the target organisation. This can be achieved through second-party audits of each vendor's technical and organisational infrastructure, ensuring they meet the required standards of cybersecurity.

QUESTIONS

Paolo Balboni
paolo.balboni@ictlc.com

Luca Bolognini
luca.bolognini@ictlc.com

Floriana Francesconi
floriana.francesconi@ictlc.com

Francesca Tugnoli
francesca.tugnoli@ictlc.com

Francesco Capparelli
francesco.capparelli@ictlc.com

Andrea Sudano
andrea.sudano@ictlc.com

ICT Legal Consulting
Milan, Rome, Bologna, Amsterdam, Athens, Madrid, Paris, Helsinki and Melbourne
www.ictlegalconsulting.com

Read more from this firm on Lexology

QUESTIONS

The Inside Track

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

Amidst the rapid growth of the digital security market, there's a rising demand for skilled and updated cybersecurity experts. Such expertise requires an unwavering commitment to professional development, given the ever-evolving landscape of cybersecurity threats and solutions. It calls for multidisciplinary skills, including a firm understanding of privacy regulations, in-depth technological knowledge and excellent communication abilities. Beyond technical competence, the capacity to articulate complex cybersecurity matters to diverse stakeholders is crucial. Cybersecurity specialists must not only comprehend the current landscape but also possess foresight to navigate future challenges.

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

The GDPR necessitates that organisations uphold the principle of accountability. As such, technological advancement must be orchestrated in harmony with international standards and GDPR mandates, embodying the principles of 'privacy by design' and 'privacy by default'. This implies that privacy considerations must be integrated into the architecture of systems and processes from their inception, ensuring a robust cybersecurity framework that respects data privacy, minimises risk and is prepared for the dynamically changing threat landscape.

How is the privacy landscape changing in your jurisdiction?

The Italian privacy domain has been revolutionised through the implementation of two pivotal legal instruments: the General Data Protection Regulation (GDPR) and the ePrivacy Directive. These have posed significant challenges to various organisational entities, both public and private, with regards to personal data protection. However, they also represent a significant stride towards the comprehensive modernisation of EU privacy rules. The integral role of robust cybersecurity measures in ensuring data privacy becomes increasingly apparent. It is a call to action for organisations to adopt a proactive approach to data protection.

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

The Clusit Report 2023 – March 2023 Edition paints a stark picture: the frequency of global cyber-attacks has experienced a significant rise compared to the previous year, coupled with a concerning escalation in their severity. Europe, in particular, has seen a notable increase in attacks. This trend underscores a strategic shift in cybercriminal tactics, from indiscriminate attacks to more specific, targeted ones. The report also stresses the recurring role of human error in data breaches, underscoring the critical need for comprehensive staff training in cybersecurity best practices. The findings serve as a potent reminder that cybersecurity extends beyond the realm of IT, demanding robust, organisation-wide strategies to safeguard business integrity.

Photo by Blue Planet Studio on Shutterstock

Japan

Tetsuya Oi, a partner at TMI Associates, is well versed in professional practices in various industrial fields, including the protection of personal information, EU data protection regulations, information security cloud services, internet content, internet of things, artificial intelligence, advertising technology and development of system applications.

Satoshi Murakami, a partner at TMI Associates, specialises in data protection, intellectual property law, internet-related law and consumer-related laws, among other fields. In particular, he has continuously represented and advised numerous domestic and international companies primarily in the technology, telecommunications, video game, e-sports, media and e-commerce industries.

Shunsuke Terakado, a partner at TMI Associates, specialises in data protection, cybersecurity, IT transactions, technology disputes involving massive data breaches, system integration projects and IP licensing. He is a iegistered information security specialist and provides advice based on both his legal and his technological knowledge.

Shohei Suzuki, an associate at TMI Associates, specialises in privacy and security law and other internet-related laws, as well as mergers and acquisitions. He has substantial experience in privacy issues relating to advertising technology and acquisitions of companies holding personal data of internet users. He is licensed to practise in both Japan and California.

QUESTIONS

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

The cybersecurity requirements applicable to most companies operating in Japan are those stipulated in the Act on the Protection of Personal Information (APPI). The APPI requires companies to take necessary and proper measures to prevent leakage, loss or damage of personal data, and to provide other security control of personal data. Guidelines issued by the Personal Information Protection Commission (PPC) explain what companies should do in order to comply with the requirements of such measures. According to the guidelines, a company is required to implement organisational, personnel, physical and technical security control measures. The guidelines make it clear that appropriate security control measures can differ from company to company, so a company should determine its appropriate security control measures while considering expected impacts on the rights and interests of data subjects in the case of data breaches as well as the possibility of data breaches.

The June 2020 amendments to the APPI, which include several important changes, came into full effect on 1 April 2022. With regard to cybersecurity requirements, the following three changes should be noted.

First, the penalty for the failure to implement appropriate security control measures has been strengthened. Under the Act prior to the amendments, a company that receives a corrective order from the PPC for failing to take appropriate security control measures and then fails to obey that order could be subject to a fine of up to ¥300,000. However, under the amended law, the upper limit of the fine is ¥100 million, and officers and employees who fail to obey the order can also be subject to a fine of up to ¥1 million or imprisonment for up to one year.


Tetsuya Oi


Satoshi Murakami


Shunsuke Terakado


Shohei Suzuki

> "A business must promptly ... notify the PPC once a data breach comes to their notice."

society, thereby contributing to the national security of Japan. This Act mainly stipulates the basic principles of Japan's national cybersecurity policy and the responsibilities of the national government, local governments and other concerned public parties. It requires businesses to make voluntary and proactive efforts to ensure cybersecurity, but there is no penalty for failing to fulfil this requirement.

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?

As mentioned in question 1, the 2020 amendment to the APPI came into full effect on 1 April 2022. The amended APPI requires businesses to report breaches of personal data to the PPC and affected data subjects when the data breaches involve actual or possible breach:

- of sensitive personal data;
- of personal data where unauthorised use of the data is likely to cause financial damage;
- that may have been caused with a malicious purpose; or
- where more than 1,000 data subjects are affected.

A 'data breach' here includes not only leakage of personal data, but also loss of and damage to personal data.

A business must promptly (ie, within around three to five days) notify the PPC once a data breach comes to their notice. Furthermore, the business must file a complete report to the PPC within 30 days or, if the data breach is likely to have been caused with a malicious purpose, within 60 days. Both reports must be made online through the PPC website by submitting a report form available on the same website.

Notices to the affected data subjects also need to be made in a timely manner depending on the situation after the business comes to know of the data breach. Businesses will be exempted from this reporting requirement if there is a situation that makes the reporting to the data subjects difficult and the business takes substitute methods to protect their rights and interests. For example, if a business does not have contact information of the affected data subjects, it does not need to provide notices to them but must publish the fact of the data breach and respond to inquiries from the data subjects.

When a company handles personal data on behalf of another entity under an entrustment agreement, both parties are subject to the notice obligation upon the event of a data breach. However, the entrusted party will be exempted from the obligation if it reports the data breach to the entrusting party.

In addition, a report is not required in the following cases:

- an advanced encryption method is adopted for the leaked information;
- all the leaked information is recovered before a third party can view it; or
- the business has a complete copy of the personal data that was lost or damaged.

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

When suffering a data security incident, the main issues that companies need to address from a privacy perspective are conducting a prompt and appropriate incident response, and ensuring accountability and transparency to data subjects and other stakeholders.

While companies have been increasing their use of data, such as by acquiring and analysing internet browsing history and location data for marketing purposes, major data security incidents attracting public attention have occurred in Japan in recent times. For example, there was unauthorised access to a mobile payment service and the service was scrapped just one month after its debut as the company struggled to resolve the security issues and restore the trust of its users. This incident reaffirmed that data breaches can have a significant impact on businesses and that preparing for incident response including accountability and transparency to data subjects is extremely important for business continuity.

Although the incident response procedure and security measures to be taken by companies may vary depending on the individual data security incident, there are a number of procedures that are usually recommended in the event of a data security incident, to prevent the spread of damage and ensure transparency and accountability to data subjects and other stakeholders.

Photo by ESB Professional on Shutterstock

First, immediately verify the facts concerned, including the causes of the data security incident and the scope of data that has been leaked. Then, immediately announce the accurate facts and express sincere apologies to data subjects – do this at an early stage, as a first and quick announcement. Immediately, make a first quick report to the PPC and other related authorities depending on which industry the company belongs to. Next, continuously announce and report to data subjects and the relevant authorities the facts that may be revealed from subsequent investigations. Perform investigations, including digital forensics, conducted not only by internal members, but also by a third-party committee consisting of specialists (including attorneys and technical specialists) who are in neutral positions to perform investigations. Security management measures must be planned based on the results of the investigations performed, to prevent any recurrence of the data security incident. Finally, the company must report the results of the investigations performed and the security management measures to prevent any recurrence of the data security incident, and it must implement the security management measures.

> "The APPI requires companies to take necessary and proper measures to prevent the leakage, loss or damage of personal data."

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

There is no single best practice to improve cybersecurity preparedness for all businesses in Japan. Generally, the security management measures to be taken by companies should be determined through self-assessment taking a risk-based approach. Accordingly, it is important to duly carry out certain processes for improving cybersecurity preparedness:

- collect the latest cybersecurity-related information and trends;
- figure out the current status of the company's security management measures;
- carry out a risk assessment and establish security management measures in accordance with the results of the assessment; and
- operate appropriately.

Since there are laws, regulations and guidelines providing a baseline that can help companies to conduct this type of assessment, we will consider them to provide an example here.

First, as we mentioned earlier, the APPI requires companies to take necessary and proper measures to prevent the leakage, loss or damage of personal data and to provide other security controls for personal data. The guidelines issued by the PPC explain what companies should do to comply with these measures. According to such guidelines, a company is required to implement organisational, personnel, physical and technical security control measures. In addition, the amended APPI requires companies to make the information about their security measures available to data subjects. Furthermore, the Financial Services Agency has issued additional guidelines that stipulate matters that require companies in the financial sector to take particularly strict security control measures in light of the nature and use of personal data in the financial sector.

Second, the Ministry of Economy, Trade and Industry has published the Cybersecurity Management Guidelines that are intended for companies that are utilising IT-related systems or services. The guidelines describe managerial strategies from the perspective of protecting companies from cyberattacks and recommend companies to implement security management measures that are based on three principles that the manager of a company should be aware of and 10 significant items that a manager of a company should instruct to the officer responsible for executing information security measures (eg, the chief information security officer who is in charge of supervising information security within the company).

Third, the Japan Institute for Promotion of Digital Economy and Community (JIPDEC) operates an assessment system for certifying whether or not the information security management system (ISMS) of a company is consistent with international standards (the ISMS conformity assessment system). Under this assessment system,

examinations are made as to whether or not an ISMS implemented by a company is in conformity with JIS Q 27001 (ISO/IEC 27001). In addition, the JIPDEC also operates a PrivacyMark System to assess companies that take appropriate measures to protect personal data.

Fourth, the Centre for Financial Industry Information Systems (FISC) has established the 'FISC Security Guidelines on Computer Systems for Banking and Related Financial Institutions' to promote security measures on financial institution information systems. These guidelines have been voluntarily observed by most financial institutions in Japan.

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

Cloud hosting services are currently in use in a wide variety of situations in Japan. However, there are some points that should be considered by business operators upon using cloud hosting services.

The APPI regulates the transfer of personal data to third parties in countries outside Japan. Many of the cloud hosting services that are widely used in Japan are operated by service providers in foreign countries. If a foreign cloud service provider processes personal data in the cloud (ie, the cloud service provider accesses personal data managed by a user, a business operator in Japan and extracts some data linked with such personal data), then the user is subject to personal data transfer regulations. Under the APPI, if personal data is transferred to a third party in a country outside Japan, the transferring party is generally required to obtain the prior consent of the relevant individual for such cross-border transfer. However, it is not practicable to obtain consent from the individuals upon using a cloud service.

Photo by f11photo on Shutterstock

One of the exceptions that is widely used is where the third party is located in a foreign country that the PPC determines and prescribes by its rules as providing an equivalent level of protection of personal data as Japan (which is currently only the European Economic Area and the United Kingdom). Another exception is where the relevant third party has established, and continues to utilise, an equivalent level of protective measures as those that are required under the APPI, which can be met by entering into appropriate agreements between the user and the cloud service provider.

Thus, in cases where the cloud service provider processes personal data in the cloud, the provider must process such personal data in Japan or meet one of the above exceptions.

In addition, in cases where the cloud service provider processes the personal data in the cloud, the user shall supervise the processing of personal data by the cloud service provider. Thus, upon choosing a cloud service, the user needs to validate the appropriateness and security of the cloud service provider.

"Japan will continue to push forward with measures to ensure 'a free, fair and secure cyberspace'."

In contrast, if the cloud service provider and the user enter into an agreement whereby the provider undertakes not to access the personal data in the cloud, and the provider actually limits the accessibility of the personal data, the provider is not regarded as processing the personal data in the cloud and is therefore not subject to the personal data transfer regulations. However, the user is fully liable for any incidents in the cloud in this case. Thus, it is important for users of cloud services to validate the appropriateness and security of the cloud service provider in this case as well.

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

The increasingly established nature of technologies in cyberspace, such as AI, the internet of things, fintech, robotics, 3D printers, and AR and VR, has seen the expansion of cybersecurity threats.

The Basic Act on Cybersecurity enacted in 2014 provides for the basic policy for cybersecurity. Under the Act, the government provides its Cybersecurity Strategy (the latest of which was made in 2021). The strategy shows the basic position and vision on cybersecurity, and objectives and implementation policies for the coming three years.

The Cybersecurity Strategy states that cybersecurity must be ensured for all people, business sectors, local regions, etc, and, in response to digitalisation, Japan will aim at ensuring cybersecurity 'with no one left behind'. Japan will continue to push forward with measures to ensure 'a free, fair and secure cyberspace' in an increasingly uncertain environment based on the following three approaches.

Simultaneously advancing DX and cybersecurity

The covid-19 pandemic and the establishment of the Digital Agency in September 2021 accelerated the digitalisation of the economy and

society in Japan. Japan will continue to promote digitalisation along with efforts to ensure cybersecurity.

Ensuring the overall safety and security of cyberspace as it becomes increasingly public, interconnected and interrelated

Japan will deepen and enhance the approaches taken in the previous cybersecurity strategy formulated in 2018 (ie, it will deepen mission assurance and enhance efforts related to risk management) and work to improve the environment and address the causes of cybersecurity threats.

Enhancing Initiatives from the perspective of national security

Japan will strengthen its defence capabilities by securing the nation's resilience through the enhanced capabilities of the relevant government institutions. At the same time, Japan will enhance its deterrence capabilities to detect, investigate, and analyse cyberattacks so that Japan can identify the attackers and hold them accountable.

In addition, numerous laws impose criminal sanctions regarding cybersecurity threats. For example, the Act on Prohibition of Unauthorised Computer Access prohibits spoofing, security loophole attacks and phishing as unauthorised computer access. In addition, the Penal Code prohibits the unauthorised creation or provision of electromagnetic records of unauthorised commands that do not operate in accordance with other persons' intention or that act against their intention, typically computer viruses.

Photo by Sean Pavone on Shutterstock

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

What are the privacy and data security risks in mergers and acquisitions?

Legal due diligence should be performed to mitigate privacy and data security issues in mergers and acquisitions from the perspectives that:

- as the importance of data increases, buyers may engage in mergers and acquisitions in order to use the data held by the target company after the acquisition; and
- the need to perform legal due diligence from a data security perspective is high, and if the data held by the target company cannot be utilised after the acquisition, the purpose of the merger and acquisition will not be achieved.

QUESTIONS

QUESTIONS

> "The buyer will need to check whether it can use the target company's data after the acquisition."

What aspects of legal due diligence need to be performed?

The first aspect is how personal data held by the target company can be used after the acquisition. The second is whether the target company's data security system is sufficient. In addition, there may be cases where potential security risks remain at the target company.

What points should be checked in terms of use of data?

If a buyer acquires a target company because it perceives the data owned by the company as being valuable, the buyer will need to check whether it can use the target company's data after the acquisition.

For example, when a food manufacturer acquires a company that operates a recipe website, the question is whether the food manufacturer can use the personal data of users visiting the recipe site. In this case, the legal due diligence should include checks to find out whether the personal data held by the target company is lawfully collected and whether the buyer can use the personal data held by the target company after the acquisition.

As regards the latter point, the question is whether the purposes of use after the acquisition are covered by the purposes of use held in the target's privacy policy before the acquisition. If this is not the case, it is necessary to obtain consent from the users before using their data for new purposes.

What points should be checked in terms of data security?

Check whether the target company has established a security system for personal data and whether it has experienced any data breach incidents.

In particular, it is very important to check whether there are any potential data breach incidents and to have the seller represent and warrant that there have been no such incidents. If the buyer overlooks potential data breach incidents and also fails to obtain the representation and warranty from the seller, the buyer can be found solely responsible for incidents once they are revealed.

Tetsuya Oi
toi@tmi.gr.jp

Satoshi Murakami
smurakami@tmi.gr.jp

Shunsuke Terakado
sterakado@tmi.gr.jp

Shohei Suzuki
ssuzuki@tmi.gr.jp

TMI Associates
Tokyo
www.tmi.gr.jp

Read more from this firm on Lexology

QUESTIONS

The Inside Track

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

Laws and regulations in the cybersecurity area include not only the APPI, but also the Unfair Competition Prevention Act, the Basic Act on Cybersecurity and other regulations and guidelines, and it is necessary to be familiar with all of these. However, often legal regulations alone are not enough to deal with actual cases. It is important for lawyers to be familiar with the latest threat information, security incidents from other companies and the technologies used to combat these, and to be able to give appropriate legal advice to clients.

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

The APPI is unique in many ways, so it is not correct and is actually quite risky for foreign companies to assume that they can automatically comply with Japanese privacy laws by simply complying with the privacy laws of their home country, such as GDPR. In particular, when it comes to the disclosure of personal data to third parties, the APPI is quite strict. A business must obtain consent from data subjects even when the recipient is an affiliate company unless an exception such as joint-use exception applies. In addition to the uniqueness of the law, the cultural differences can make it difficult for foreign companies to prepare for the privacy issues. In Japan, receiving a recommendation or investigation from the authority itself can have a huge negative impact on a business.

How is the privacy landscape changing in your jurisdiction?

The APPI was amended in 2017, and this amendment introduced a rule that the APPI would be reviewed every three years as in the plan, do check act cycle. The PPC has issued administrative guidance and corrective instructions in some cases where it found inappropriate processing of personal data. In addition, the APPI was amended in June 2020 in accordance with the said cycle, with the amendments that came into effect on 1 April 2022, and under such amendment a monetary sanction was increased up to ¥100 million. We believe the regulatory environment for personal data will become stricter than it currently is, and businesses should be more cautious about data processing.

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

In Japan, companies need to be most careful of massive data breaches caused by ransomware attack. Japan's Information Technology Promotion Agency ranked ransomware attack as the top threat in 2022 and 2023. For their protection, companies must establish an organisational framework, develop a security policy and incident response workflows, manage information and educate employees as well as maintaining backups to be prepared in case of database encryption. They also need to be aware of security incidents caused by advanced persistent threats, information leaks by internal fraudulent acts and compromised business email systems.

Photo by Dmitry Morgan on Shutterstock

Netherlands

Quinten Kroes heads Brinkhof's data protection practice and has been active as a lawyer in the telecommunications, media and technology (TMT) sectors since 1995, advising on and litigating matters of telecommunications, media and data protection law. He advises a broad range of companies on data protection. He has supported various companies that have been the subject of investigations by the Dutch Data Protection Authority.

Quinten's reputation is recognised as top tier in legal directories, as is the quality of Brinkhof's data protection practice.

Quinten Pilon is an associate at Brinkhof and specialises in data protection, TMT and competition. He advises clients on a broad range of data protection and cybersecurity-related issues.

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

In terms of new legislation, several amendments in the field of cybersecurity are noteworthy. At the national level, an amendment to the Dutch Network and Information Systems Security Act law entered into force on 1 December 2022, which allows the National Cyber Security Centre (NCSC) to share information about cyber threats with the private sector. Previously, the NCSC was only allowed to inform and advise vital providers and government bodies with up-to-date threat and incident information about their network and information systems. Under the new system, 'linchpin organisations' can receive threat and incident information from the NCSC. These linchpin organisations can in turn share that information with their constituencies. An example of such a linchpin organisation is the Digital Trust Centre, part of the Ministry of Economic Affairs and Climate. Other linchpin organisations serve specific constituencies, such as the healthcare or high-tech sectors. Additionally, the NCSC can now also share threat or incident information directly with non-vital providers. This is allowed if there is no linchpin organisation that can provide the non-vital provider with the information and the information concerns a threat or incident with potentially significant consequences for the continuity of the provider's services.

On 18 April 2023, the Dutch legislator also approved the proposal for the (Dutch) Act on Electronic Data Interchange in Healthcare (Wegiz). The Wegiz stipulates that healthcare providers may be required to exchange certain data in electronic form. While the Wegiz regulates how data should be exchanged, it does not regulate whether the healthcare provider is allowed to exchange the data nor the types of data that can be exchanged. What data is exchanged between healthcare providers is determined by the healthcare providers themselves. The Wegiz is expected to enter into force on 1 July 2023.

At the European level, the NIS2 Directive entered into force on 16 January 2023. The NIS2 Directive has widened the scope of the first NIS Directive, introducing a size-cap rule covering medium and large-sized entities from a large variety of sectors. The Directive also applies to some critical and essential entities regardless of their size. Key material changes include detailed rules for incident-reporting, stricter enforcement requirements, the harmonisation of sanction regimes across member states and improvement of cooperation between member states. There is now a two-year period during which all member states must implement the NIS2 Directive's measures into their national legislation.

The Digital Operational Resilience Act (DORA) also entered into force on 16 January 2023 at the EU-level. This regulation creates a firm regulatory framework for digital operational resilience in the financial sectors, by introducing rules for the protection against, and

> "The Dutch DPA will not shy away from using its GDPR powers to go after the violation of other fundamental rights, such as the right to equal treatment."

the detection, containment and recovery of ICT-related incidents. Importantly, DORA does not merely apply to financial institutions, but also to 'ICT third-party service providers'. These are non-financial service providers that provide third-party ICT services to financial institutions. DORA constitutes a lex specialis in relation to the NIS2 Directive. Companies will have a two-year period to prepare for DORA, as its provisions will apply from 17 January 2025.

Aside from these new laws, the main regulatory development has been that the enforcement of the GDPR, by both the Dutch regulator and through collective class action claims, is steadily increasing. So far, the Dutch data protection authority (DPA)'s preferred method of enforcement seems to be the imposition of administrative fines. Cases where it has decided to impose an order or a ban on the processing of personal data, or issued a formal warning or reprimand, are the exception. So far, the Dutch DPA has published 22 fines that it imposed on both companies and government institutions for violating the GDPR. Three of these fines were imposed for a failure to notify a data breach in a timely manner and six fines for failing to implement sufficient security measures. With regard to collective class action claims it is noteworthy that the Court of Justice of the European Union recently ruled that mere infringement of the GDPR does not give rise to a right to compensation. However, the court also affirmed that the right to compensation is not limited to non-material damage that reaches a certain threshold of seriousness. Member states with minimum thresholds for non-material damages, such as the Netherlands, will therefore likely have to accept separate liability regimes for such damages under the GDPR.

Generally, the fines published by the Dutch DPA have been relatively high compared to fines imposed on average in other member states, although not near the level of the highest. The Dutch DPA imposed two record fines of €3.7 million and €2.75 million on the Dutch Tax Administration for illegally processing personal data in its fraud identification facility and for discriminatory and unlawful data processing respectively. Although both cases were quite unique and have also triggered a broader political and societal debate on racial profiling and discrimination, it shows that the Dutch DPA will not shy away from using its GDPR powers to go after the violation of other fundamental rights, such as the right to equal treatment. In concrete terms, it will take violations of other fundamental rights into account in determining the fine for the violation under the GDPR. The Dutch DPA has also imposed fines on relatively small organisations, which are significantly lower than what its fining guidelines suggest. For example, an orthodontic practice was fined €12,000 for insufficiently securing the personal data that patients were uploading to its website. Similarly, lower fines were imposed on a small foundation aligned to a Dutch political party, and an outdoor advertising company that had failed to adequately protect certain HR records.

Several fines that the Dutch DPA imposed have now been challenged in court. In one case, the district court in Utrecht ruled that the Dutch DPA had wrongly rejected the 'legitimate interest' as basis for

the processing of personal data by a company that offered amateur football clubs a platform to film and stream matches. In doing so, the court rejected the Dutch DPA's official position that purely commercial interests can never qualify as a 'legitimate interest'. Moreover, in appeal the Council of State ruled that the platform for amateur football did not have a purely commercial interest, but also a social interest. In another case with a similar question of law, the Amsterdam District Court has referred preliminary questions to the European Court of Justice. In this case, a tennis association had provided personal data to a third party for a fee, without seeking the consent of its members. The referring court has asked whether a purely commercial interest and the interest as at issue here, the provision of personal data for payment without the consent of the data subject, can be regarded as legitimate interests, and if so under which circumstances. Finally, the district court in The Hague found that a fine on a local hospital for its failure to implement adequate access restrictions to patient records was justified, but that the amount of €460,000 was unreasonably high. The court lowered it by €110,000, mainly because the hospital had taken a number of measures to prevent further violations.

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?

Pursuant to article 33 of the GDPR, a controller must notify a personal data breach to the Dutch DPA, unless the breach is unlikely to result in a risk to the rights and freedoms of natural persons. If the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller must also, without undue delay, inform the data subjects, communicating in clear and

Photo by Alexey Fedorenko on Shutterstock

plain language the nature of the personal data breach (article 34 GDPR). This communication is not required when the controller has taken measures to ensure that the risk of a breach is not likely to materialise. Breach notification requirements similar to those contained in the GDPR already existed in Dutch law since 2016.

The European Data Protection Board's (EDPB) has published guidelines 9/2022 with general guidance on personal data breach notification under GDPR, as well as a separate set of guidelines (01/2021 on Examples regarding Personal Data Breach Notification) with concrete examples of the types of incidents that should be notified. The Dutch DPA also publishes informal guidance on this topic on its website, including its own list of concrete examples.

All these documents make it clear that a number of criteria will be relevant to assess whether a notification needs to be made. These include the sensitivity of the data, the number of data subjects affected, the volume of data lost and the possible consequences for data subjects. Moreover, it is also considered relevant to take into

account who received the information and to which categories of data subjects the data relate (eg, data relating to children or other vulnerable groups).

The Dutch DPA has also given further guidance on its website specifically on whether ransomware can qualify as a breach that needs to be notified. In short, it takes the position that this is indeed the case, as the illegal encryption of data implies illegal access to data and a circumvention of security measures that should have prevented this. The guidance issued in 2021 by the EDPB confirms this approach. The Dutch DPA also considers that it will often be hard to establish the precise effects of ransomware and to exclude the risk that it may have transferred or manipulated personal data in addition to encrypting the data. The Dutch DPA has stated that paying a ransom to (supposedly) prevent criminals from further spreading personal data after a ransomware attack, does not exempt organisations from notifying the personal data breach to Dutch DPA or data subjects. It does not consider paying ransom an appropriate measure that will prevent high risks to the rights and freedoms of data subjects to materialise. After all, paying a ransom does not guarantee that hackers will actually delete (and not resell) all personal data.

"The Dutch DPA has stated that paying a ransom to (supposedly) prevent criminals from further spreading personal data after a ransomware attack, does not exempt organisations from notifying the personal data breach to Dutch DPA or data subjects."

In the case of doubt, the Dutch DPA recommends to submit a preliminary notification of a possible breach. The notification can always be amended or even withdrawn at a later time, when the controller has more knowledge of the breach and its consequences. Controllers can notify through a web-based notification tool on the Dutch DPA's website, which was updated in 2021. Currently, this tool is only available in Dutch. However, an English language questionnaire, which includes all questions of the online notification tool as well as some explanatory comments, is available on the website of the Dutch DPA.

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

Companies must continuously assess both the technical and the organisational measures they are taking to protect and secure their personal data. If a security incident occurs the company should give priority to fixing the particular security issue and do its utmost to mitigate the negative consequences of the breach.

Measures to be taken will vary depending on the type of incident, from trying to locate a lost data carrier, to contacting the recipients of an email that was wrongly sent or addressed, remote wiping of a portable device or working with a processor to establish the extent of a security incident in their domain. A recent court ruling confirms that processors may even be ordered by a court to provide detailed information on security incidents if they fail to do so in response to legitimate customer queries. If a hacker may have obtained personal data, the company will have to assess whether or not the data had been sufficiently encrypted, as this is relevant to the question whether a notification should be made. If passwords have been leaked, the company should force users to change these passwords.

A data breach could be an indication that existing organisational and technical measures are not adequate. Maintaining appropriate and adequate levels of security requires continuous efforts and constant scrutiny through risk assessments, planning, executing, checking and doing the same all over again (the 'plan-do-check-act' cycle (PDCA)). The guidance adopted by the EDBP in 2020 on privacy-by-design and privacy-by-default confirms this. This is a logical consequence of the notion that the adequacy of measures must be viewed in light of current technical standards. It does not necessarily mean that technical measures need to be renewed at least annually to match the most advanced security system available. However, at least a suitable

Photo by Dmitry Morgan on Shutterstock

level of proactive monitoring is required: when imposing a fine on the Dutch Employee Insurance Agency (UWV) in July 2021, the Dutch DPA took into account the fact that the UWV did not sufficiently monitor and evaluate its security measures.

The strength of the measures should also be viewed in proportion to the nature of the data it protects. A pizza shop with a spreadsheet of local customer addresses for mailing promotional flyers will not need military-level encryption. But processing of sensitive data will require measures like two-factor authentication, encryption, hashing (both using state-of-the-art algorithms) and/or, if possible, anonymisation or pseudonymisation.

The Dutch DPA considers two-factor authentication to be a common and fairly easy security measure to implement. Increasingly, organisations turn two-factor authentication on by default. According to the Dutch DPA, two-factor authentication is a minimum requirement for securing access to health data. Moreover, it should be borne in mind that the Dutch DPA not only considers the special

categories of personal data as defined in the GDPR sensitive. In the past, it has also recognised other categories of data, such as location data and data concerning someone's media consumption, as sensitive in nature. Failure to comply can have consequences. The DPA has imposed a fine on an airline company for not implementing strong passwords and two-factor authentication in its back office systems, which contributed to a data breach.

Organisational measures to be applied include confidentiality agreements with employees, disabling access to personal data for employees who have no need to use the data, adequate contracts with data processors and the deletion of records at the end of their retention period. Access to data should be logged and the resulting logs reviewed regularly. Adequate measures should also include clear documentation and instructions on what actions to take if an incident occurs. Timing is important; as the Dutch DPA's fine of Booking.com in 2021 shows, professional parties are expected to meet the timelines set out in the GDPR. If the cause and consequences of an incident are not yet clear, companies are advised to file a preliminary notification with the Dutch DPA, and to err on the side of caution.

A recent fine by the Dutch DPA for a local bank furthermore shows that proactive action after a data security incident can significantly reduce a fine following a security incident. The bank was fined due to a data breach caused by poor identity verification by the telephone helpdesk. However, shortly after the incident the bank compensated the affected data subjects and submitted a comprehensive risk inventory and action plan to the Dutch DPA. Subsequently, the bank at its own initiative swiftly implemented a large number of improvement measures relating to their recording practices, system support, testing and assurance, and to increase their internal professionalism and awareness in this field. The Dutch DPA also noted that despite the breach of article 32 GDPR, the bank had taken some prior measures

"A recent fine by the Dutch DPA for a local bank furthermore shows that proactive action after a data security incident can significantly reduce a fine following a security incident."

QUESTIONS

to minimalise the privacy risks for data subjects. This prompted the Dutch DPA to reduce its fine from €310,000 to €150,000.

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

As with any other modern networked society, the Netherlands is very much dependent on digital infrastructure. Statistics by the NCSC show that the vast majority of cyberattacks concern phishing, ransomware and denial-of-service attacks, all of which require vastly different remedies. As a direct consequence of this diversity, the NCSC advises a varied approach. However, as a general observation it can be noted that research shows that it is essential to increase individuals' security awareness, which will not only benefit their security practices at home but also the security of the companies they work for. Updated software and regular backups (patch management) and the need for strong passwords are also essential to resilience against cyberattacks. Using professionally secured cloud services is among the general advice given to companies to increase their security. Large companies are, of course, better equipped to meet the cybersecurity challenges and may also rely on external experts to become more resilient against cyberattacks. The EDPB, however, has recently published a data protection guide specifically for small business, which gives clear and step-by-step instructions for achieving GDPR-level data protection, including practical tips for improving security standards. In general, the NCSC advises companies to divide user accounts into low-, medium- and high-impact accounts, depending on the sensitivity of the data that the account contains and the resources that the account has access to. The report advises to implement more stricter security measures for medium- and high-impact accounts. With regard to ransomware attacks, the NCSC has published guidance entitled Ransomware

Photo by photo.ua on Shutterstock

Incident Response Plan. This explains how organisations can contain a breach, fix a vulnerability, remove the malware and prevent unauthorised access in the future by following the incident response cycle (Preparation-Identification-Containment-Eradication-Recovery-Lessons learned). Moreover, the NCSC has recommended that organisations scale up network capacity to be able to serve the large number of homeworkers, which has become more normal since the covid pandemic, and imposing appropriate security safeguards. These include forcing the use of a secure connection to the corporate network through, for example, a virtual private network (VPN), making maximum use of multi-factor authentication and enforcing strong passwords. Furthermore, the Dutch DPA has also provided useful guidance to workers on how to work securely from home. It has advised them to only work from a secure work environment, to protect sensitive documents, to use (video)chat services cautiously and to be on the alert for phishing mails.

QUESTIONS

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

The controller is, and will, remain responsible and liable for any personal data he or she collects or processes. An important aspect of cloud services is the location where personal data is actually stored and processed. Under the GDPR, personal data may only be processed outside the European Union (or more precisely: the European Economic Area (EEA)) if the third-country where the data is processed provides an adequate level of protection. Compliance can be achieved in various ways, all having to do with ensuring that adequate safeguards are in place within either the company or the country to which the data is transferred.

However, the EU Court of Justice's ruling invalidating the European Commission's EU-US Privacy Shield approval in the case of *Schrems II* has shown that safeguards in the context of international data transfers can be fragile. *Schrems II* has had far-reaching consequences beyond the Privacy Shield alone, as it also forced data exporters to conduct so-called transfer impact assessments (or TIAs) for data transfers based on standard contractual clause (SCCs) s, and to assess whether 'additional measures' are necessary to guarantee an adequate level of protection. In doing so, this judgment has called into question the legitimacy of international data transfers to not only the US but also to other destinations outside the EEA. The Recommendations of the EDPB that followed it unfortunately do not offer easy solutions for all transfer scenarios either.

Currently, the main way to transfer personal data to the US on a regular basis is by concluding SCCs combined with implementing (individual) transfer impact assessments. The recently adopted SCCs by the European Commission – which had to be implemented by 27

"The controller is, and will, remain responsible and liable for any personal data he or she collects or processes. An important aspect of cloud services is the location where personal data is actually stored and processed."

December 2022 – go some way to address the concerns raised by *Schrems II* and contain updated clauses that are aligned with the GDPR. Yet these SCCs can only be relied on by organisations that transfer personal data to non-EEA parties that are not subject to the GDPR. As the larger US-based cloud providers will likely fall under the territorial scope of the GDPR, organisations will, strictly speaking, not be able to rely on the updated SCCs as a transfer mechanism to these cloud providers. The European Commission has, in the meantime, clarified that it is in the process of creating new SCCs for transfers to non-EEA parties that are subject to the GDPR.

Possibly, this uncertain situation will be redressed by the adoption of the new EU-US Data Privacy Framework (DPF). President Joe Biden signed an Executive Order on 7 October 2022 outlining what steps the United States will take to implement the commitments as set out in agreement in principle on the new DPF. The Executive Order includes safeguards to the processing of personal data by US intelligence authorities by limiting the access to data to what is necessary and proportionate to protect national security and the establishment of an independent and impartial redress mechanism. However, the Executive Order faced criticism, including from the European Parliament. This has taken the position that the Executive Order is not sufficiently in line with the *Schrems II* criteria, causing the DPF to be vulnerable to a new legal challenge. It is currently unclear when the DPF will be implemented. Transfers to the UK remain lawful without the need to implement any transfer mechanism, due to the adequacy decision the Commission adopted on 28 June 2021. However, this too could be reconsidered if the UK were to implement changes to its data protection framework.

These developments raise the question whether data localisation is in fact the only robust and long-term solution likely to withstand future legal challenges. With respect to cloud services in general, the Dutch DPA has published a number of guideline that are in line with

Photo by fokke baarssen on Shutterstock

the former article 29 Working Party's guidance on the issue and that do not raise fundamental obstacles to the nature of cloud computing. For example, the Dutch DPA has taken the view that, even for medical data, there is no need to ask consumers for specific permission for the use of cloud hosted services. But there are also looming signs of a more restrictive view. In January 2022, the DPA published a disclaimer on its manual for privacy-friendly settings of Google Analytics, stating that it is considering a complaint on this cloud-based website analytics tool, which may lead it to conclude that Google Analytics may no longer be used lawfully in the Netherlands. Since then, however, the Dutch DPA has not provided any further comment on this matter.

While this indicates a general openness to cloud solutions for now, using cloud hosting will need to be part of the overall risk assessment the controller makes before moving to the cloud, and one that may need to involve a data protection impact assessment under the GDPR. The Dutch government has itself commissioned various DPIAs into governmental use of commercial cloud services. Interestingly, these DPIAs focus heavily on the processing of diagnostic data by service

providers (ie, data about the use of their cloud services, rather than the data provided by customers). The final reports, which are all available online in English, have guided the government's negotiations with a number of large international cloud providers, and have, for example, prompted Microsoft to amend its privacy policy worldwide. Last year, the Dutch government signed an agreement with Google Cloud that also includes enhanced privacy measures. As a result Dutch government agencies can continue to use Google Workspace in compliance with the GDPR.

Risk assessment does not stop once the choice has been made for a particular cloud solution: if the cloud host faces security issues, the controller will need to rethink using this particular company. A first indication of the quality of the host may be found in the availability of certificates (ISO, ISAE, NEN) concerning security. According to article 28 GPDR, adherence to an approved code of conduct may also be used to demonstrate sufficient guarantees. In 2020, the Dutch DPA approved the code of conduct submitted by NL Digital, an association of IT companies, including cloud providers. Similar codes of conduct have been approved at the EU level, most notably the CISPE Code of Conduct and the EU Cloud Code of Conduct.

To assist controllers and processors to determine what 'appropriate technical and organisational measures' (article 34 GDPR) are, the European Union Agency for Network and Information Security (ENISA) has published guidelines that with examples of such measures. ENISA has emphasised that the guidelines do not have a 'legal status', and mainly serve as guidance for market parties. The NCSC shared its own experiences in moving to the cloud, which is intended to help other organisations. In addition, the NCSC published a factsheet containing five general tips for procuring secure cloud-hosting services.

Contractually, it is advisable to address any specific concerns a controller may have in the processor agreement proposed by the

"Risk assessment does not stop once the choice has been made for a particular cloud solution: if the cloud host faces security issues, the controller will need to rethink using this particular company."

cloud provider. The controller should ensure that the contract allows for access to the data at all times, even in a situation of conflict with the processor. The processor agreement should also address the issue of data location explicitly, as this is a specific requirement under the GDPR and one that may be particularly challenging to address in a cloud-based setting. Other topics that warrant careful deliberation are the provider's duty to support the notification duty of the data controller if a breach should occur in the cloud provider's domain, the provider's transparency on issues like law enforcement cooperation and also the provider's role in processing metadata about the use of its services.

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

The NCSC was established in 2012. This public–private body advises companies and the government on the usage of software and measures to increase cybersecurity. Its aim is to make the Netherlands more resilient against cybercrime.

In its Cybersecurity Assessment Netherlands (CSAN) 2022, the NSCS concluded that digital risks to Dutch national security remain high. The gravest threats are posed mainly by state actors, cybercriminals and outages. While the Netherlands has taken steps towards more resilience against cybercrime in the past year, the 2022 CSAN reiterates that the current level of resilience is still insufficient. According to the report there is a growing gap between the extent of the threats and the level of digital dependence as compared to the resilience of society against these threats. All too often, even basic measures have still not been implemented sufficiently, such as the use of multi-factor authentication and reliable backup systems. The NCSC notes major differences between various sectors and organisations when it comes to their digital resilience. Organisations

Photo by Luca Santilli on Shutterstock

that are sufficiently resilient have not only implemented basic security measures but have also focused on a risk-based method of working.

In order to resist cybersecurity threats, the Digital Trust Centre (DTC) was founded in December 2020 to help increase the resilience of businesses against digital threats. Also, the NCSC joined the so-called LDS, a platform in which both public and private parties, the NCSC and the DTC exchange information and knowledge about cybersecurity. This cooperation supports a more intensive information exchange between the NCSC and affiliated parties. Aside from the NCSC, there is also the National Coordinator for Security and Counterterrorism (NCTV). This government agency was established in 2012. Its aim is to protect Dutch society against disruptive security threats. NCTV monitors and coordinates initiatives from the public, private and public–private sectors to strengthen cybersecurity in the Netherlands. Cooperation between the General Intelligence and Security Service, the Dutch Military Intelligence and Security Service, the NCSC, the police and the public prosecutor has also been further strengthened. Additionally, the Dutch government appointed its first

Secretary of State for Digitalisation in January 2022, whose agenda for 2023 includes topics such as the improvement of digital literacy, combatting the spread of disinformation and the development of a quality mark for algorithms.

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

Companies are well advised to conduct thorough due diligence on a target's IT environment and previous experience with security incidents, which should be logged internally as a requirement of law under the GDPR. The occurrence of a security incident need in itself not be worrisome. The response of the company to the incident can be much more telling about the company's readiness and level of compliance.

When it comes to privacy and personal data, we note an increased emphasis on compliance in the context of due diligence for M&A deals. This increased emphasis is evident in various different ways. First, target companies are investigated with more scrutiny for their GDPR compliance. Second, more thought is given to the GDPR aspects of the transaction itself, such as resulting data transfers or changes to intended use of data. This, no doubt, has everything to do with the risk presented by the enormous fines that can be imposed under the GDPR for non-compliance.

There is also an increased awareness among competition authorities about the importance of vast collections of data and their potential monetary value, even if this is not necessarily reflected by equally large market shares. The Dutch competition and consumer rights authority has also highlighted the collection of data by online platforms as a potential source of market power and the Ministry of Economic Affairs and Climate Policy has suggested that upcoming mergers and acquisitions should be reviewed based on deal value instead of the historic turnover of the companies involved. It is also noteworthy that last year the Dutch parliament has agreed on a new act (Wet VIFO) regulating investments in critical sectors, such as energy, logistics, finance and sensitive technology. The act introduces a notification obligation and requires authorisation from the Dutch Ministry of Economic Affairs and Climate.

QUESTIONS

Quinten Kroes
quinten.kroes@brinkhof.com

Quinten Pilon
quinten.pilon@brinkhof.com

Brinkhof NV
Amsterdam
www.brinkhof.com

Read more from this firm on Lexology

QUESTIONS

The Inside Track

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

A thorough understanding of cyber threats and the capability to work with relatively new and untested legal regimes. This requires an open mind, curiosity and creativity, and sometimes a healthy dose of paranoia about the threats. It is also important for the lawyer to have a technical interest or background, to help in bridging the cultural divide between IT specialists and the legal and compliance teams.

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

The Netherlands is a relatively tech-savvy country, with clients approaching us with innovative and challenging legal questions. Our data protection authority has also always taken a keen interest in new technical developments such as mobile apps, facial recognition software and Wi-Fi tracking in public spaces. It has taken aggressive stances on issues such as cookie consent and legitimate interests.

How is the privacy landscape changing in your jurisdiction?

The impact of the GDPR on the Dutch society is significant. Cybersecurity has become an increasing concern, and it has become a clear priority for the current government based on its coalition agreement. The Dutch DPA is also set to receive more funding. Aside from public enforcement, there is also a growing risk of private enforcement: the Netherlands is a venue of choice for GDPR-related collective damage cases.

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

The Dutch DPA notes an increase in the amount of hacking, malware and phishing in the data breach notifications it receives. It therefore stresses the importance of using multiple factor authentication, and warns of malicious techniques such as social engineering, password spraying and credential stuffing. For its part, the NCSC continues to warn companies about the exploitation of VPN vulnerabilities by state actors and criminals.

Photo by Suradech Singhanat on Shutterstock

Switzerland

Jürg Schneider is a partner at Walder Wyss and 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 focus on transborder and international contexts. He frequently publishes and lectures in his areas of focus.

David Vasella is a partner and co-head of the regulated markets, competition, tech and IP team. He advises Swiss and international clients on a wide range of IT and data protection matters, including compliance implementation projects, and provides clear and actionable advice on issues such as data protection, data monetisation, analytics, secrecy obligations, cloud outsourcing arrangements and advertising law. He frequently publishes and lectures in his areas of focus.

Hugh Reeves is a managing associate in the regulated markets, competition, tech and IP team. He advises clients in matters of technology transactions, commercial contracts, telecommunications, intellectual property and digitalisation. 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.

QUESTIONS

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

Cybersecurity is a hot topic in Switzerland. Although the number of cyberattacks is consistently growing each year, many commentators have highlighted the fact that companies incorporated in Switzerland as well as public bodies tend to underestimate or mismanage – either through a lack of clear information or of proper legal incentives – the risks posed by cybersecurity. As a result, these organisations are not sufficiently prepared to combat and withstand cyberthreats.

In light of the above, the Swiss government has been putting some effort in recent years in raising awareness among the industry and helping organisations in moving towards better cybersecurity preparedness.

At first, the Federal Council (the federal executive body) adopted a national strategy for the protection of Switzerland against cyber risks (NCS). This strategy was set up to implement a variety of measures to improve cybersecurity awareness and preparedness, one of them being the creation of a centralised cybersecurity body at the federal level, the National Cyber Security Centre (NCSC). This new organisation aims to create a nationwide response to cyberthreats and serves as a unified contact point for the industry.

On another level, the Swiss parliament adopted a new Federal Act on Data Protection (FADP) on 25 September 2020. This new law will enter into force on 1 September 2023. In many areas, the revised FADP has been aligned with the provisions of the General Data Protection Regulation (GDPR) applicable in the EU. However, the Swiss law does often not go into the same level as detail as its EU counterpart. Nevertheless, the revised FADP does contain its own material specificities, not the least of which is the existence of sanctions for individuals (ie, not the legal entity itself) in the event of violations of


Jürg Schneider


David Vasella


Hugh Reeves

"Many companies active in Switzerland also fall under the scope of the GDPR."

Photo by SCStock on Shutterstock

the data protection provisions. It should, however, be borne in mind that many companies active in Switzerland also fall under the scope of the GDPR, because of the orientation of their activity towards the European Economic Area (EEA). Contrary to its predecessor, the revised FADP contains express notification duties for data security breaches (see hereafter).

In addition, the Federal Council suggested, in December 2020, to introduce a breach notification obligation in cases of cybersecurity incidents affecting critical infrastructure on the grounds that perpetrators of cyberattacks often use similar methods and patterns for critical infrastructure in different sectors. This breach notification obligation could thus significantly enhance the cyber resilience of critical infrastructure by quickly identifying attack methods and transmitting corresponding alerts. This notification obligation is expected to enter into force in the course of 2023 as part of the Information Security Act of 18 December 2020 (ISA). The ISA regulates information security practices within the federal government and its administrative bodies. The ISA is the basis for several ordinances to further specify and implement information security requirements.

QUESTIONS

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?

As of 1 September 2023, and in contrast to the previous FADP, a data breach notification duty will apply in a broad set of cases. According to the new FADP, the data controller is required to inform the Federal Data Protection and Information Commissioner (FDPIC) – the Swiss data protection authority – of any data security breach that could potentially result in a high risk to the personality rights of the data subjects. To this extent, Swiss law is expected to be somewhat more lenient than EU law, as the threshold for informing the FDPIC will be higher ('high risk' v 'risk'). The processor must however inform the controller of any data security breach.

The notification must indicate at least the nature of the data security breach, its consequences and the measures taken or planned. The notification must be made as soon as possible, depending on the circumstances of the case. As a general principle, we believe that the notification period should depend on the damaging consequences of the leak. The greater the potential harm, the sooner the notification of the breach.

Furthermore, the controller must also inform the data subjects, when necessary for their protection or if specifically required by the FDPIC. This information can be restricted, postponed or waived under certain circumstances, for example, if there is a legal duty to maintain a secret, if the information is impossible to provide or requires

disproportionate efforts or if the information of the data subject can be guaranteed in an equivalent manner by public disclosure.

It is important to note that the data processor also has an obligation to notify the controller of any data security breach as soon as possible under the new law.

Under the new law, individuals who intentionally breach certain provisions of the FADP face a criminal fine of up to 250,000 Swiss francs. This is significantly higher than under the previous FADP, where breaches were sanctioned with a maximum fine of 10,000 Swiss francs – and only under certain restrictive circumstances. However, failure to report a data breach incident does not directly fall under the scope of these criminal sanctions. Accordingly, there is no criminal prosecution for a reporting duty breach under the revised FADP, though a sanction can be levied if it appears that the minimum data security requirements were not in place.

Furthermore, the FADP states that if an organisation notifies a data breach in accordance with its obligation pursuant to the new law, this notification may not be used in criminal proceedings against the person obliged to notify without its consent. The protection of the data controller is thus reinforced. This provision intends to encourage organisations to report any data security breach in compliance with the law, without having to fear for a conviction in a subsequent criminal proceeding.

An organisation failing to report a data security breach may also expose itself to a serious reputational harm if the information goes public through other channels. Therefore, organisations would generally be well advised to strictly adhere to the legal framework, which they should interpret in a prudent (ie, expansive) manner.

"There is no criminal prosecution for a reporting duty breach under the revised FADP."

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

The main issues can be subdivided into four chronological phases that a company has to go through when suffering a data security incident.

First, organisations must determine the exact cause of the data security incident. It is very important to know whether the incident is due to a technical issue or if the company was subject to a cyberattack. This will then allow the organisation to take adequate measures to remedy the data security incident (internally or with involved third parties such as storage providers). Once the cause of the incident has been identified, the organisation should also be able to assess whether the incident is over or whether it is still ongoing, as may be the case if an ill-intentioned actor revealed a back door in the company's IT systems and shared those revelations with third parties.

QUESTIONS

> "Importantly, organisations must know as quickly as possible whether data was potentially stolen, disclosed or lost. If so, the exact scope of the data incident must be clarified."

Second, but in parallel, organisations must determine the exact impact of the cybersecurity incident. Importantly, organisations must know as quickly as possible whether data was potentially stolen, disclosed or lost. If so, the exact scope of the data incident must be clarified, particularly if personal data or confidential information affecting contractual partners are impacted.

Third, under the revised FADP, if it appears that personal data or confidential information was impacted by the incident, the company's management or another designated person within the company must determine whether there is a high risk that the personality rights of the data subjects may be violated. More often than not, this will be the case at this stage, as it is rather difficult to categorically exclude the infringement of personality rights of data subjects. It should also be borne in mind that organisations are required to make a quick decision in this situation, which should lead them to admit the existence of such a risk, except in few rare cases.

Fourth, still under the new law, if there is a high risk to the personality rights of the data subjects, the company's management or another designated person within the company must decide whether or not the company should notify the data breach to the FDPIC or the data subjects themselves. Regarding the factors and risks to be considered in this respect, reference is made to the developments in question 2.

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

An initial step is to assess the level of compliance with the GDPR. Many Swiss-based companies already fall under the scope of the GDPR, given the latter's extraterritorial scope of applicability. These businesses therefore need to aim for GDPR compliance. As a result, companies in Switzerland had to bolster their data security and adopt mechanisms to

prevent data breaches in accordance with the requirements under the GDPR. That said, those organisations that already comply with EU law are largely prepared under the revised FADP as well.

Nevertheless, some adjustments may be necessary to meet the specific requirements of the revised FADP. For instance, businesses would be well-advised to perform an audit of the existing internal data protection processes or perform a specific risk assessment. This could give rise to a need to review and enhance processes, practices, documentation, contracts, policies and notices, and a need to establish new ones.

Companies should however not only focus on adopting measures to prevent the risk of cyberattacks, but also on developing internal regulations as to how to react to a data breach. Proper management of a cybersecurity crisis is more effective if organisations have clear guidelines in terms of competences and procedures. The individuals in charge must be able to follow a straightforward procedure to determine the cause of the data breach as quickly as possible and to determine whether data has been impacted or not. This gives companies a vital safety belt in a time where fast thinking and swift decisions are key.

In any event, organisations must assess on a case-by-case basis the extent to which their data protection processes need to be adjusted. Swiss companies that do not fall under the scope of the GDPR and have not implemented any changes thereunder likely need to put in additional effort towards compliance with the revised FADP.

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 services is widely accepted in Switzerland and is often a better choice in terms of data security in comparison with an internal IT storage set-up. This is because third-party cloud providers need to be constantly up to date with the latest technological evolutions to achieve adequate data security. To that extent, they can be seen as specialists in their field of expertise. In addition, cloud providers often have deep and extensive experience in the hosting area. Therefore, transferring data to a reputable cloud hosting environment is often seen as a best practice in terms of data security.

Photo by Anson Fernandez Dionisio on Shutterstock

One talked about topic is the relevance of certifications when it comes to choosing between different cloud hosting services. Swiss law imposes a general obligation on cloud providers to ensure adequate data security. For that purpose, many cloud service providers have sought to obtain data security and cybersecurity certifications, aiming to reassure potential clients that their data is in good hands. That said, certifications should still be seen mostly as a form of guidance rather than any exhaustive guarantee as to service quality. In any event, clients should also choose a cloud provider considering other factors, such as business continuity, key performance indicators and adequate support level.

QUESTIONS

On the other hand, privacy becomes a serious issue when transferring data to a cloud hosting environment, especially if the provider is located abroad in a country that is not deemed to have an adequate level of data protection in its own legal landscape. The country in which the hosting (or data access) occurs will inform any additional steps, such as conducting a data transfer impact assessment and safeguards, the parties will need to take. Failure to take these measures could qualify as a breach of the Swiss data protection legislation.

As a result, in a cloud services scenario, the parties may have to conduct a data protection impact assessment and implement additional safeguards in cases of cross-border disclosure or storage of personal data. One way to compensate for the lower level of data protection is to incorporate contractual clauses, especially the 'Standard Contractual Clauses of the European Commission', adapted to Switzerland.

In summary, the reliance on an external cloud hosting environment is, for the data controller, very much a balancing act between the numerous technical advantages, on the one hand, and the need for a correct legal assessment and set-up on the other.

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

As mentioned in question 1, the Swiss government adopted the NCS and set up the NCSC. This has primarily helped to achieve awareness among the various actors of the market regarding the risks posed by cyberattacks.

On 18 May 2022, the Federal Council took note of the report on the effectiveness assessment of the NCS and decided to create a further

"The Swiss Federal Council initiated steps towards adopting policies and regulations concerning the specific topic of cybersecurity."

25 positions in the area of protection against cyber risks. It also decided to turn the NCSC into a federal office and instructed the Federal Department of Finance (FDF) to prepare proposals by the end of 2022 regarding how the office should be structured and which department it should be part of. This demonstrates a firm intention to further strengthen the nationwide response to cybersecurity threats and criminal activity.

Moreover, the Swiss Federal Council initiated steps towards adopting policies and regulations concerning the specific topic of cybersecurity. This represents a break from the past, as cybersecurity was traditionally addressed as a subtopic of data protection and data security. The recent developments, especially the adoption of the ISA and its provisions regarding reporting obligations for operators of critical infrastructure, have shown that cybersecurity is now a focus for the Swiss government.

Despite the above, the Swiss legislative process is comparatively slow. For this reason, the current discussions surrounding cybersecurity

Photo by Pedro Costa Simeao on Shutterstock

are not expected to lead, in the short term, to the adoption of an overarching legislative act on cybersecurity standards.

Nonetheless, the absence of clear cybersecurity standards on the legislative level has paved the way for some public-private organisations to contribute to the development of a response against cyberthreats in Switzerland. For example, a private–public initiative was created under the name 'Trust Valley'. This project aims to further enhance Switzerland's position as a hub for matters of digital trust and cybersecurity. On another level, the DiploFoundation, the Federal Department of Foreign Affairs and the Federal Office of Communications joined forces to create the Geneva Internet Platform, a discussion centre for digital policy matters, including those pertaining to cybersecurity.

In addition, cybersecurity has also become a favoured topic for higher education institutions, which often have specialised centres focusing on this manner. This is, for instance, the case for the Swiss Federal Institute of Technology in Zurich (ETH), which opened a Center for Security Studies. A similar study path was launched at the Swiss Federal Institute of Technology in Lausanne (EPFL), resulting in the setting-up of the Center for Digital Trust (also known under the moniker C4DT).

Furthermore, the ETH and the EPFL have joined forces with the national defence in creating the 'Cyber-Defense Campus' under federal direction, which brings together governmental, academic and industrial actors to reflect on cybersecurity in the context of national defence.

The above-mentioned initiatives show that Switzerland is committed to promoting a solid response towards cyberthreats.

QUESTIONS

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). 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 the 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

> "Furthermore, the ETH and the EPFL have joined forces with the national defence in creating the 'Cyber-Defense Campus'."

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 the 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. A data breach could involve the loss of valuable trade secrets, such as secret recipes, client lists, production methods and so forth. Moreover, the reputational 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 breaches may lead to high fines. As these fines are calculated on the entire group turnover, acquiring a company that is still breaching data protection 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 the 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 Ltd
Lausanne and Zurich
www.walderwyss.com

Read more from this firm on Lexology

QUESTIONS

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. That 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?

First, the relevant technologies are evolving very rapidly. We enjoy following technological evolutions and catching a glimpse of tomorrow's technologies. Second, 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?

A fully revised data protection act will come into force on 1 September 2023. This new law is going to bring closer alignment to the EU's GDPR. Moreover, the ISA, which will introduce fundamental rules for cybersecurity in critical infrastructures, is expected to come into force in the course of 2023. 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 that 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.

Photo by ESB Professional on Shutterstock

Taiwan

Ken-Ying Tseng currently heads Lee and Li's digital, TMT and data privacy practice group. Before 2018, she was the head of Lee and Li's M&A practice group for 12 years. She received an LLM from Harvard Law School. Ken-Ying advises on various forms of mergers and acquisitions, and is experienced in resolving both legal and commercial issues. She assisted and represented several multinational corporations in their M&A activities, including TPG, Aleees, McDonald's, Sony, PTT, Costco and Mediatek.

In addition to M&A, Ken-Ying constantly advises various tech companies that are in the businesses of social networks, instant messengers, search engines, portal sites, sharing economy, e-commerce, OTT, online games, P2P lending, e-payments and cloud computing. Ken-Ying also frequently advises clients, including multinational companies, on privacy and data protection (GDPR), e-marketing, big data, e-signature, domain name, fintech, artificial intelligence, cybersecurity, internet governance and other legal issues.

Ken-Ying is admitted to practise law in both Taiwan and New York. She has been recognised as one of the Top Taiwan Lawyers in 2022 and 2023 by *Asia Business Law Journal*, a Distinguished Practitioner 2022 and 2023 in corporate and M&A by *Asialaw*, a Highly Regarded Leading Lawyer by *IFLR1000*, and the Most Influential Woman in Personal Data Protection Law 2019 – Taiwan by *Acquisition INTL*.

Ken-Ying holds other positions: the managing director, Taiwan Internet Government Forum, member of the International Affairs Committee of TWNIC, chair, Digital Service and Data Protection Committee, Taipei Bar Association supervisor, and supervisor of the National Information Infrastructure Enterprise Promotion Association.

QUESTIONS

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

There have not been any major developments in Taiwan with regard to cybersecurity related laws and statutes. However, given the recent surge of fraud cases as well as cybersecurity or data breach incidents, the primary regulator of cybersecurity, the Ministry of Digital Affairs (MODA) and some of the legislators from the opposition parties have been planning to propose the amendments to the Cybersecurity Management Act (the Cybersecurity Act). MODA took over the responsibility of regulating cybersecurity matters in Taiwan in August 2022.

The Cybersecurity Ac, the Enforcement Rules of the Cybersecurity Act (the Enforcement Rules), as well as may other regulations promulgated under the Cybersecurity Act, are the main laws and regulations governing cybersecurity law matters in Taiwan since 1 January 2019. Pursuant to the Cybersecurity Act and the relevant regulations, such as the Regulations for Classification of Cybersecurity Responsibility, cybersecurity responsibility is further classified into five levels (from Level A to Level E). Each government agency must stipulate its own cybersecurity maintenance plan and also set forth the guidelines on cybersecurity matters for the 'specific non-governmental agencies' that it regulates. Many government agencies have promulgated such guidelines to regulate the 'specific non-governmental agencies' subject to their jurisdiction.

Meanwhile, the primary regulator of the financial industry and listed companies, the Financial Supervisory Commission (FSC), announced its new agenda to improve cybersecurity of the companies listed in Taiwan in March 2023, aiming to further strengthen the cybersecurity of listed companies from three perspectives: (1) information disclosure, (2) corporate governance, and (3) regulatory assistance.


Ken-Ying Tseng

While the FSC has been implementing many measures from the first two perspectives over the years (for example, listed companies, depending on their sizes, are required to hire chief information security officers within certain deadlines), with regard to the third perspective, the FSC now encourages companies listed in Taiwan to participate in Taiwan Computer Emergency Response Team (TWCERT) so that the private sector can share cybersecurity information, and to introduce standard operating procedures (SOPs) such as ISO27001 and CNS27001 or to obtain certification from other third-party certification authority with regard to cybersecurity.

"Hence, as long as there is a security breach incident, even if no 'personal data' is involved, the incident may be subject to reporting requirements."

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?

Pursuant to the Cybersecurity Act, the agencies subject to the Cybersecurity Act shall report to its supervisory agency, or to the competent authority of the industry that the private agency is engaging in, as applicable when the agency becomes aware of a cybersecurity incident. A cybersecurity incident refers to any incident under which the system or information may have been accessed without authorisation, used, controlled, disclosed, damaged, altered, deleted or otherwise infringed, affecting the function of the information communication system, and thereby threatening the cybersecurity policy. Hence, as long as there is a security breach incident, even if no 'personal data' is involved, the incident may be subject to reporting requirements.

The Regulations for Reporting and Responding Cybersecurity Incidents set forth further details about the reporting of cybersecurity incident as required under the Cybersecurity Act. A 'specific non-government agency' shall report to its regulator at the central government within 'one hour' after it becomes aware of the cybersecurity incident, and the regulator shall respond within two to eight hours depending on the classification of the cybersecurity incident. In the meantime, the specific non-government agency shall complete damages control or recovery of the system within 36 to 72 hours depending on the classification of the cybersecurity incident.

Meanwhile, if personal data is involved in a data breach incident, pursuant to the Personal Data Protection Act (the PDPA), either a public agency or a non-public agency shall inform the affected data subjects of the data breach incident as soon as it inspects the relevant incident. In the notice to the data subjects, the relevant facts concerning the incidents, such as what data was stolen, when the incident happened, the potential suspect that breached the data and the remedial actions that have been taken shall be described. The PDPA does not set forth any threshold of the notification to the affected data subjects.

On the notification to the regulator, the PDPA does not specify any obligations to report a data breach incident to the regulator. However, in the personal data security maintenance plans stipulated by the competent authorities of each industry, the regulator may require the private sector to report a data breach incident to it within a 72-hour period. Thus far, the competent authorities of many industries have included the data breach incident reporting requirement in the personal data security maintenance plans that they stipulated. As a result, many industries in Taiwan are now subject to a 72-hour reporting requirement under which they shall report to their competent authority a data breach incident within 72 hours of becoming aware of the occurrence a data breach incident. In most

cases, reporting will only become mandatory when the data breach incident is deemed 'material'. Some of the competent authority has adopted its own definition of 'material', such as 'affecting the daily operation' of the private business.

Telecommunications operators are subject to an even stricter reporting requirement in the way that a report must be filed with the competent authority within one hour of a telecommunications operator becomes aware of a material data breach. Meanwhile, financial institutions shall asses if the incident materially impacts their operations. If so, they will need to report to their respective primary regulators and take responsive actions as required by the relevant regulations.

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

The most important issue for a company facing a data security incident shall be how to prevent further damage or harm that may be caused by such an incident. If possible, a company shall notify the affected data subjects as soon as possible so that they are alerted and have the chance to take precautionary measures (for example, resetting their passwords) in time. A company shall also take immediate actions to detect and fix the loophole in its system, if any, to prevent any further breach or damages.

In many of the data security incidents that are locally reported, the cause of the incident is not system failure or hackers' activity but the misconduct by the relevant employees, contractors or the employees of the contractors. Hence, it is very important for a company to adopt proper security measures and internal control rules, awareness training and standards for employees or contractor selection. Often, the data breach incident could be caused by the mistake made by

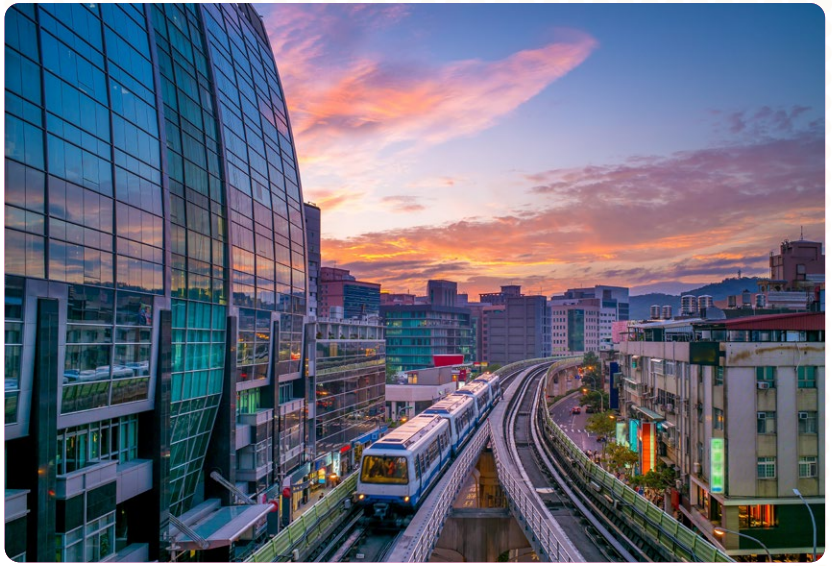


Photo by Richie Chan on Shutterstock

the staff of small service vendors, but the large companies retaining their services would be forced to deal with the customers who may suffer damages. At the end, cases would be settled because the small service vendors may not be financially capable of bearing the relevant liabilities but the large companies need to protect their brand names. Hence, a company needs to carefully select its service vendor, and in the service agreements, clauses addressing to personal data protection and indemnification liabilities shall be included.

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

In Taiwan, most of the businesses are cost-sensitive small or medium-sized enterprises, and they tend to believe that adopting a certain 'one-stop' solution (ie, installing a certain 'package software') can handle the cybersecurity issues as well as compliance of the applicable privacy laws, including the General Data Portection

QUESTIONS

"The data controller may also have administrative fines imposed for any breach of the PDPA by the data processor. Hence, it is important to select a trustworthy cloud service provider when a business decides to move its data to the cloud."

Regulation (GDPR). This is, of course, not the case. Even purely from an IT perspective, installing package software may not be sufficient in protecting the businesses from cyberattacks.

Large corporations are more cautious and normally will hire IT specialists or consultants or lawyers to implement security measures, to conduct internal training and to design SOPs, etc. They will also seek internationally recognised certifications, such as ISO27001. Some of the industries are required to pass ISO27001 certifications, such as the telecommunications industry.

Companies may also consider joining certain alliances, such as the TWCERm, to obtain or share intelligence in relation to recent cybersecurity threats and relevant resources.

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

Pursuant to the PDPA, a cloud service provider will most likely be deemed as a data processor, while the business using the cloud service will be deemed the data controller. Pursuant to the PDPA, the data controller shall be held liable to its customers if the cloud service provider or data processor does not comply with the PDPA or the instruction of the data controller. The data controller may also have administrative fines imposed for any breach of the PDPA by the data processor. Hence, it is important to select a trustworthy cloud service provider when a business decides to move its data to the cloud.

The business shall also check whether it is subject to any special sector regulations for outsourcing data processing or storage or even storing data outside of Taiwan. For example, financial institutions are subject to the prior approval of the competent authorities for

outsourcing activities. The regulatory approval in this regard is rather burdensome. Furthermore, for some industries, customers' data are prohibited from being stored in China, such as telecommunications operators and TV channels, cable TV system operators, social worker firms and human resources agencies.

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

The websites and systems of the Taiwan government, as well as large corporations, have been frequently hacked or attacked by attackers outside of Taiwan, such as from China. The cyber army of China was blamed for most of the attacks and incidents. Meanwhile, incidents involving 'fake news' or misinformation that is distributed by Chinese on Taiwanese websites have been one of the major combats that the Taiwan government is fighting against. To protect the cybersecurity of Taiwan, the Executive Yuan initiated a series of actions, including the implementation of the Cybersecurity Act. By imposing the relevant requirements under the Cybersecurity Act, such as strengthening the regulated agencies' internal procedures and SOPs, the Taiwan government aims to raise cybersecurity standards in Taiwan and the ability to fight against cyberattack. The government also hopes to foster the growth of the local cybersecurity industry through the implementation of the Cybersecurity Act as there will be more audit tasks to be conducted by the regulatory agencies.

Recognising that cybersecurity is national security, the Taiwan government amended its National Security Act in 2019, claiming and explicitly stating that the protection of national security shall include the protection of the security of cyberspace, as well as physical space, in the territory of Taiwan.

Photo by Nambaman on Shutterstock

With regard to the prevention of criminal activities, the Taiwan government has long-established a special task force, the 9th Investigation Corp of the Criminal Investigation Bureau, to combat criminal activities conducted via high-tech or information technology, such as computer crime, cybercrime, and so on. All of the cyber-related crime activities reports will be forwarded to the 9th Investigation Corp for further investigation. The 9th Investigation Corp is equipped with police officers with technology backgrounds as well as high-tech hardware and software. It has established channels with police authorities in other countries to investigate cross-border crimes. To combat phone fraud activities, the National Police Agency further established a special phone line, '165', to assist the general public in fighting against the fraudsters. Recently, MODA has also been strengthening its investigation into e-commerce operators for their alleged failure to protect the personal data of their users.

QUESTIONS

> "The acquirer or surviving entity shall also estimate the costs to fix the existing issues and to reform the operation."

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

An acquirer or surviving entity in an M&A deal needs to evaluate the potential risks from the following perspectives.

The first perspective is the track record of the target. Past records of data breach incidents, and notable non-compliance of privacy laws, can be used to evaluate the existing or contingent liabilities of the target, as well as the pattern for future potential liabilities in the event that the target continues its operation in the same manner after the M&A.

The second is data ethics. If the target constantly ignores cybersecurity threats or disrespects privacy or data ethics, there may be unpredictable contingent liabilities already.

The third is costs for future reform. In addition to the liabilities evaluation stated above, the acquirer or surviving entity shall also estimate the costs to fix the existing issues and to reform the operation. This will include the costs for: (1) IT, (2) obtaining proper consents from the data subjects, and (3) performing notification obligations to the data subjects.

The fourth is the losses to be incurred due to reduction of customer database. Customer data without proper consents would need to be eliminated and the losses of business opportunities shall also be considered and calculated.

Ken-Ying Tseng
kenying@leeandli.com

Lee and Li, Attorneys At Law
Taipei
www.leeandli.com

Read more from this firm on Lexology

QUESTIONS

The Inside Track

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

The lawyer must have sufficient experience, knowledge and training before he or she takes on the case so that the lawyer would be able to navigate you through the troubled waters. This lawyer needs to have the ability to think and act fast as a cybersecurity incident could be evolving hours by hours or even minutes by minutes. This is a particular area of law where it is not affordable to train the lawyer with whom you frequently consult if this lawyer does not have any practical experiences in this field. Furthermore, a cybersecurity incident may not be handled merely from a legal perspective, and sometimes, you would need to deal with government relationship as well as public reputation or relationship. The lawyer needs to be able to take all of the relevant factors into consideration when rendering advices.

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

I found cybersecurity and privacy practices fascinating because I would encounter cutting-edge legal and commercial issues and need to respond instantly. 'As soon as possible' may not be sufficient. I will have to address all of the potential legal liabilities and consequences to the clients as well as remind the client of all of the compliance reports, filings and actions all at once within a very short time frame. I also need to be creative in order to guide the client to take the best approach to encounter the situation.

How is the privacy landscape changing in your jurisdiction?

Taiwan adopted a legal framework of personal data protection that is similar to the EU data protection laws. Some of the provisions are even stricter, and Taiwan is one of the very few countries without a centralised data protection authority. Taiwan has submitted its application for a GDPR adequacy decision in 2018 and is in the process of negotiating with EU. The Executive Yuan of Taiwan adopted its first reforming bill of the PDPA in April 2023 to establish an independent agency regulating data privacy matters and increase the penalties for failure to comply with the data security obligations, and these new amendments were enacted on 16 May 2023. A preparatory office for the new independent agency governing personal data protection matters is expected to be set up by 1 August 2023.

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

Since the pandemic period, the number of cybersecurity incidents as well as fraud cases soaring. It has become the Taiwan government's primary target to combat fraud cases as well as cybersecurity risks and threats. MODA, and the other sectoral regulators, are actively exercise their power to launch the relevant investigations and urge the private sector to further strengthen their cybersecurity abilities. Meanwhile, given the surge of fraud cases, the Taiwan government formed special taskforce to combat the relevant fraud activities, including amending the PDPA and other statutes.

Photo by fedjason on Shutterstock

United Kingdom

Peter Dalton is a technology lawyer at Stephenson Harwood with over a decade of experience in the fields of technology disputes, cyber-security and technology-focused intellectual property. His holistic technology practice allows him to provide comprehensive advice on complex and at times 'bet the company' cyber mandates. Peter has considerable experience advising on the full range of cyber advisory, incident response and litigation matters, often on a global basis. He has acted for large multinationals, financial institutions and household names in respect of pre-incident legal preparation and policies, incident response, regulatory advice and regulator engagement. His experience in cyber response and crisis management has focused on complex business-critical incidents including nation-state espionage, ransomware attacks and BEC fraud. He also advises clients in respect of litigation arising from incidents, as part of his wider technology disputes practice, which centres on complex licensing disputes, distressed projects, and software development and audit disputes.

Katie Hewson is a data protection partner who leads the firm's data protection practice. She has significant experience advising clients across a variety of sectors. Recently awarded Privacy Leader of the Year: Legal (PICASSO Privacy Awards 2022), Katie is recognised as a Next Generation Partner for data protection, privacy and cybersecurity by *The Legal 500 UK* 2023. She is also ranked as an Up and Coming Lawyer for data protection and information law in the *Chambers and Partners UK* 2023 guide. She has extensive experience leading international GDPR compliance projects and also advises on data protection contracts, cybersecurity and personal data breaches. She also advises a variety of clients on direct marketing, ad tech, social media and cookies issues under the e-privacy regime.

QUESTIONS

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

The increasingly tense international situation has been the driving force for many developments over the past year. In addition, as the UK is no longer in the EU, lawmakers and regulators in the UK are no longer bound to follow EU regulatory changes and this year has seen the start of a divergent approach.

For example, while the EU has announced the repeal and replacement of the Cyber Security Directive ((EU) 2016/1148) (also referred to as the Network and Information Systems Directive or NIS Directive) with new, wider and more prescriptive regulations known as NIS2, the UK government has decided to go in a different direction. Following a public consultation into proposals to improve the UK's cyber resilience, the UK government announced that it would retain the UK's NIS Regulations (NIS), which are the UK's implementing regulations (enacted pre-Brexit) for the EU's Cyber Security Directive, but with some modifications. The main proposed changes (which are unlikely to take place before 2024) amount to: (1) including IT managed service providers (MSP) within the entities regulated by NIS in the UK; and (2) putting in place provisions to allow NIS to be updated more easily in the future, using secondary legislation. The government has stated that it will continue to look at reforms that it proposed in the consultation but that it has yet to decide on, for example, whether to expand notification requirements under NIS to capture incidents beyond those causing service disruption.

The expansion of NIS to cover MSPs makes sense given the importance of the sector to swathes of the UK economy. An attack on an MSP has the potential to impact its corporate and governmental customers across the economy, as well as exposing the data that they host for those clients, making them high-profile targets for attackers.

This has been demonstrated by the number of attacks by criminal and nation-state affiliated groups in recent years, most recently seen with the high-profile attack on the UK headquartered outsourcer, Capita, which has been attributed in the press to the Black Rasta ransomware group.

These changes are less comprehensive than those being implemented in the EU via the repeal of NIS and replacement with NIS2, which expands more substantially the sectors brought under NIS, reduces notification time limits in the event of an incident, and sets out the minimum-security obligations required in more prescriptive detail. The UK government's position is that its more nuanced changes allow for flexibility and an industry-specific approach, tailored to the UK economy and highlighting 'outcome focused tools', such as the National Cyber Security Centre's (NCSC)

> "The UK will not be subject to the EU's proposed Cyber Security Resilience Act."

Cyber Assessment Framework, which provide a measure of flexibility for companies.

Like the EU, the UK is also looking at 'internet of things' products and the cyber risk they pose (ie, products that connect to the internet). The UK will not be subject to the EU's proposed Cyber Security Resilience Act, which will impose EU-wide security rules on manufacturers, importers and distributors of 'connected products', enforcing minimum security standards for such products. Instead, following a public consultation, the UK intends to introduce security requirements for such products as part of the Product Security and Telecommunications Infrastructure Bill, which received Royal Assent in 2022. The Bill introduces a regime that is intended to codify certain security obligations and standards for such products, where currently there is only a code of practice published in 2018, which is not mandatory. As with the EU law, the government intends such obligations to be applicable to manufacturers, importers and distributors of connected products but, unlike the EU law, the Bill only applies to consumer products (which includes any product that is sold both to consumers and business users). Further, we do not know the detail of the security obligations that will be imposed, or how far they will diverge from their EU counterparts, because the underlying obligations will be published as part of secondary regulations that the government intends to implement under the powers granted by the Bill; it has not published a timetable for doing so, and has said it will give manufacturers, importers, and distributors 12 months' grace from the implementation of such regulations before they enter into force.

Finally, we would note that while there has been much discussion regarding the changes to the UK GDPR that the government proposed in the Data Protection and Digital Information Bill (No. 2), introduced into parliament in March 2023, the current proposals do not include changes directly applicable to cybersecurity standards.

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?

There are various regulations in force in the UK covering different parts of the economy; in an incident response situation, organisations need to be aware of the regulations that apply to them and be able to assess whether the relevant threshold has been met accordingly. In all cases, organisations need to be able to assess the impact of the incident on an ongoing basis, which requires close coordination between legal teams and forensics, IT and the wider business so that decisions can be made at pace as new information becomes available. Key obligations arise as follows:

- The UK GDPR requires data controllers to notify the Information Commissioner's Office (ICO) where a data breach relates to

personal data, unless the incident is unlikely to pose a risk to the rights or freedoms of individuals. This notification must be made within 72 hours of becoming aware of the breach. UK GDPR also requires data controllers to notify impacted individuals where the breach is likely to result in a high risk to their rights and freedoms. Such notification is to be made 'without undue delay'. This involves assessing the nature of the data impacted by an incident, the likelihood that it has been accessed or exfiltrated by unauthorised parties, the persons to whom the data relates and the harm that could be caused by such data to the data subjects impacted on a case-by-case basis.

Data processors that process personal data on behalf of data controllers are not required to notify the ICO or data subjects where they suffer a data breach, but they are required to notify the relevant data controller without delay; the data controller is then subject to the above obligations regarding notifications to the ICO and individuals.

- Entities that provide public electronic communications services (such as telecommunications operators and internet service providers) must notify personal data breaches to the ICO within 24 hours of becoming aware of the data breach. Providers can, where necessary, provide initial information within the 24-hour window with the full set of information required under the relevant rules to be provided within three days. If the data breach is likely to adversely affect subscribers or users, the service provider must also notify them without undue delay. These requirements come from the Privacy and Electronic Communications regime, which is composed of the Privacy and Electronic Communications (EC Directive) Regulations 2003 (SI 2003/2426) (PECR 2003) as amended in 2011, and the UK Notification Regulation, the retained EU law version of Commission Regulation (EU) No. 611/2013 on the measures applicable to the notification of personal data breaches under the E-Privacy Directive (2002/58/EC).

Photo by William Perugini on Shutterstock

In addition to the above regulations that specifically concern data breaches, organisations may have other notification obligations to regulators or the public, based on the nature of the breach. These often arise from sector specific regulations or rules, and include:

- Regulated entities in the financial sector may have to notify the FCA under Principle 11 of the FCA Handbook, which requires notification of any matter in respect of which the FCA would reasonably expect notice. FCA guidance has stated that this includes notifying it of any significant failure in a firm's systems or controls, which is understood to include cyber incidents and data breaches.
- Publicly listed entities may need to put out market announcements where an incident may impact the share price, which could include a significant data breach.

QUESTIONS

"Organisations need to ensure that legal advisers are properly in touch with the situation to advise on the regulatory obligations upon the organisation and when there is sufficient information to trigger notification obligations."

- Entities regulated by NIS need to notify their regulator (which varies depending on sector) where an incident disrupts continuity of service. This requirement is not a direct consequence of a data breach, but rather of any incident impacting service provision. Under NIS, regulated entities must notify the regulator within 72 hours of becoming aware of the incident.
- Professional and regulated firms may have obligations to their industry regulators; for example, a solicitors' firm would need to notify the Solicitors Regulation Authority.

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

Organisations face numerous concerns from a privacy perspective when they suffer a cyber incident. These include:

- Containing the incident to prevent further data impacts.
- Establishing internal and external control groups and key stakeholders to make decisions.
- Ensuring communications concerning the incident are secure; this may involve using alternative communication methods if there is a concern that internal email is compromised.
- Establishing as far as possible that privilege is maintained given the risk of future litigation.
- Alongside third-party experts and internal IT resources, establishing the extent of data impacted, whether it is personal data, the data subjects impacted, and the seriousness of the breach for those data subjects. This is inevitably a moving picture as the incident evolves, and organisations need to ensure that legal advisers are properly in touch with the situation to advise on the regulatory obligations upon the organisation and when there is sufficient information to trigger notification obligations.

- Ensuring that impacted data subjects are treated in accordance with regulatory and legal obligations and with a view to minimising and where possible remediating potential harm caused by the incident (for example, by offering credit monitoring services).
- Ensuring that communications regarding the incident made to data subjects, employees, stakeholders, the press, on social media or to any other third party, are consistent with legal and regulatory obligations, and with the organisation's incident response strategy. This will require coordination between external legal, PR and forensics advisers, and key internal stakeholders.
- Having in mind the potential for litigation in the future and, where consistent with legal and good practice obligations, preparing for such possibilities.

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

Like the EU, UK regulation generally requires organisations to have in place suitable organisational and technical measures with regard to the nature of the threat posed. Precise regulatory obligations depend on the regulation that the organisation is subject to, but in broad terms organisations need to ensure sufficient measures are in place on both the technical and the organisational side. Best practices include implementing a full suite of technical, legal and operational incident response plans, stress testing these with tabletop exercises on a regular basis and providing full training across the organisation to ensure implementation. Organisations often work with third-party providers such as forensic and IT experts, law firms, security and penetration testers, PR firms, to ensure that their measures and responses are appropriate and highlight inconsistencies or learning points and do so on a regular and repeating basis.

Photo by Boris Stroujko on Shutterstock

The imperative to develop strong cybersecurity preparedness is increasingly commercial as well as risk based. Corporate transactions such as M&A deals or investment rounds will increasingly look at cyber resilience as part of their due diligence, PE houses are paying more attention to resilience in portfolio companies, and a general 'hardening' of the insurance market has meant that those seeking insurance must demonstrate minimum security standards, such as having implemented MFA across their estate, to both obtain coverage and ensure recoverability in the event of a loss.

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

Businesses need to ensure that cloud providers adhere to sufficient security standards to ensure that data is held securely and safely and that they have proper recourse in the event of an incident. This is

not least because using a cloud provider will not in any way absolve them of responsibility to data subjects, customers or any other legal liability, in respect of the data for which they are responsible. They will want to conduct suitable due diligence to ensure that the cloud provider is reputable and has proper security in place. Some businesses will hold sufficiently sensitive data to warrant requiring cloud providers to provide special or heightened security in respect of that data. The reality is that, in many cases, businesses may struggle to negotiate meaningful changes to cloud providers' standard terms (although organisations with greater bargaining power, or that are obtaining cloud storage as part of wider more bespoke IT projects, may be able to do so). In any event, organisations should scrutinise the cloud providers' terms and provisions to ensure that the contract contains meaningful contractual obligations in respect of data security, that they have sufficient oversight of the cloud provider's performance, and that the contract provides means by which they are to be provided with such information and control as they require in the event of a cyber incident in order to fulfil their legal obligations. They will also want to ensure there are sufficient warranties and indemnities to protect them if the cloud provider suffers an incident that causes the organisation loss, and that the limits and exclusions of liability are suitable and do not render large portions of their potential losses irrecoverable.

Organisations will also need to think about the location of the providers' data centres, and whether using such providers will engage data transfer regulations under UK GDPR or otherwise (one reason that many cloud providers' offer EU-located data centres to UK and EU organisations).

"Organisations should scrutinise the cloud providers' terms and provisions to ensure that the contract contains meaningful contractual obligations in respect of data security that they have sufficient oversight of the cloud provider's performance."

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

The UK government is taking steps to try to maintain and improve the cyber resilience of both government and the wider economy through a combination of regulation, technical assistance and various industry-specific codes of conduct. The approach it generally seeks to adopt is one of flexibility; rather than impose top-down security standards from the centre, cyber resilience regulation in the UK generally tends to be sectoral, with regulations targeted at certain sectors (generally those deemed more critical to the UK from a technical or systemic risk perspective) and regulatory oversight often delegated to sector-specific regulators. It tends to adopt an outcome-focused approach, as seen in its proposals to reform rather than replace NIS, a departure from the approach being taken by the EU. Cybersecurity policy in the UK falls within the remit of the Department for Culture, Media and Sport, which also sponsors and operates a series of cyber-related schemes, codes and training events aimed at specific sectors and parts of the UK economy.

Technical risk in the UK is managed by the National Centre for Cyber Security (NCSC), a part of GCHQ. The NCSC provides advice, guidance and support on cybersecurity, including the management of cybersecurity incidents, as well as providing threat intelligence to and for the government in an effort to combat cyber threats targeting UK organisations. The NCSC has also produced a series of toolkits and guides to help raise cyber awareness in the UK.

These bodies sometimes come together to pursue policy objectives. For example, the Information Commissioner's Office (ICO) (the data protection regulator) and NCSC recently wrote a joint letter to the Law Society, noting that the payment of a ransom would not be taken into account as a risk mitigation measure by the ICO when considering

Photo by ZGPhotography on Shutterstock

whether to take enforcement action over GDPR breaches relating to cyber incidents. The intention apparently is to discourage payment by encouraging law firms to advise their client of the ICO's position when it comes to ransom payment.

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

Companies need to be aware that mergers and acquisitions can bring a whole new area of data protection and cyber risk. The target acquisition or merger partner will have its own IT systems, personnel, data holding and retention practices, and risk profile. In some cases, the buyer may be planning to integrate the target into its own business, thus potentially importing any risk inherent in the target into its own environment. Buyers need to perform proper due diligence so that they understand the level of risk they are taking on

QUESTIONS

and the current data protection and cyber hygiene of the target and can mitigate any issues, either before or after the transaction. Targets need to ensure that they have prepared properly so that they are able to give comfort to potential buyers as to the standard of their cyber and data resilience. Where disclosure during due diligence shows that an incident occurred in the past, buyers will want to investigate fully to understand the cause of the incident, whether it was contained properly, the remediation undertaken to prevent repeats, and whether there remains any legal risk associated with the incident. Where an incident has led to ongoing legal (or technical) issues that have yet to be resolved, buyers will want to ensure that the likely costs are understood and catered for as part of the transaction (although it is notoriously difficult to estimate overall exposure, especially for larger, global incidents). The buyer should assess and take into account the risk of the target's personal data processing activities within its overall assessment of the deal.

"Targets need to ensure that they have prepared properly so that they are able to give comfort to potential buyers as to the standard of their cyber and data resilience."

Peter Dalton
peter.dalton@shlegal.com

Katie Hewson
katie.hewson@shlegal.com

Stephenson Harwood
London
www.shlegal.com

Read more from this firm on Lexology

QUESTIONS

The Inside Track

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

Lawyers in the cyber space need to be able to guide clients through highly stressful and demanding situations that many clients will not have experienced before. There is a significant crisis management aspect to cyber response, which lawyers need to be able to help clients with. Cyber lawyers also need to have a strong understanding of the technical underpinning of cyber issues; the law and regulatory landscape can only be understood in light of this, and in a breach situation the forensic investigation will be a critical driver of the legal response. Finally, cyber lawyers need to be able to appreciate and understand a wide range of legal issues and have a holistic view of the client's business.

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

The UK is a relatively mature jurisdiction as regards data privacy and cybersecurity law; however, the law is fragmented in the sense that cybersecurity and incident response rules are dispersed across regulatory regimes. While the UK GDPR applies to all organisations, there are cyber-relevant laws contained in many sector-specific regulations, laws and industry groups, and different types of business are subject to different regulators.

Further, UK case law is constantly evolving as claimants and defendants seek to raise novel arguments to advance or defend claims relating to data protection and cyber issues. Good practice is also not static; lawyers must constantly adapt and develop strategies to help clients in an ever-changing threat landscape.

How is the privacy landscape changing in your jurisdiction?

The UK is seeking to amend both its data protection laws and its approach to interpreting retained EU law precedents post-Brexit. This creates some uncertainty, but also makes data protection and privacy a dynamic area to advise on. The UK's approach seeks to encourage innovation and to draw on its practical experience of the EU GDPR, while taking advantage of the UK's relative agility in amending its national laws.

Recent uncertainty around transferring personal data internationally has also seen the UK at the forefront of initiatives to create international multilateral data transfer frameworks.

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

The rising volume and cost of ransomware has been the big story of recent years. We are also seeing criminals becoming more inventive in their attempts to extort payments. Companies need to be aware of the risk and ensure that their technical and organisational measures are in order and consistent with the threat they face. Insider risk is also an increasing issue. Finally, the explosion of generative forms of AI is adding an additional source of potential threat as criminals use AI to craft phishing emails, write malware and otherwise enhance their capabilities.

Photo by Songquan Deng on Shutterstock

United States

Jason Chipman is a WilmerHale partner who advises companies on complex regulatory matters associated with data security, cyber incident response, the Committee on Foreign Investment in the United States and related export controls. He has assisted companies in most sectors of the economy on data security best practices and frequently assists with corporate due diligence. Mr Chipman currently serves as a non-resident fellow at the National Security Institute.

Benjamin Powell is a WilmerHale partner who has advised companies on major cybersecurity incidents and preparedness across virtually every sector, including banking, investment management, retail, defence and intelligence. He is recognised as a leading attorney in international investment and mergers, including the Committee on Foreign Investment and the Defense Security Service.

Arianna Evers is a WilmerHale special counsel who advises clients on complex privacy, data security and consumer protection issues. She helps clients with cybersecurity incident preparedness, incident response and internal investigations, and regulatory inquiries relating to data security breaches.

Shannon Togawa Mercer is a WilmerHale senior associate who advises clients on matters related to cybersecurity, privacy, and US and European data protection. She advises a broad range of clients in cybersecurity incident response and preparedness. She joined WilmerHale from the London location of a large global law firm where her practice focused the cybersecurity and data protection aspects of capital markets transactions and mergers and acquisitions.

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

The trend toward more proscriptive cybersecurity requirements in economic sectors perceived as playing a critical role in the US economy or for US security continues. For example, in March 2022, the Cyber Incident Reporting for Critical Infrastructure Act of 2022 was signed into law, requiring critical infrastructure entities to report material cybersecurity incidents and ransomware payments to the Cybersecurity and Infrastructure Security Agency (CISA). Additionally, in April 2022, a final rule issued by the Office of the Comptroller of the Currency, the Board of Governors of the Federal Reserve System and the Federal Deposit Insurance Corporation took effect, which requires banking organisations and their bank service providers to report any significant cybersecurity incident within 36 hours of discovery. The Securities and Exchange Commission has also proposed rules that are intended to enhance disclosures about cybersecurity risk management, strategy, governance and incident reporting by public companies and has recently proposed updates to Regulation S-P that would, among other things, impose new cyber incident response requirements and burdens on covered institutions with respect to the handling of consumer data and information. The New York Department of Financial Services has also proposed amending its cybersecurity regulation, 23 NYCRR Part 500, which would impose greater compliance obligations on covered entities.

Many of these developments align with both President Biden's Executive Order on Improving the Nation's Cybersecurity (the Cybersecurity EO) and subsequent executive actions, which set out to improve cybersecurity, particularly in relation to federal government systems. They also align with the White House National Cybersecurity Strategy released in March 2023, replacing the 2018 National Cybersecurity Strategy, focusing on privacy sector accountability and,

> "Federal agencies are likely to continue efforts to aggressively police cybersecurity regulatory compliance applicable to particular economic sectors."

in part, on shifting liability to manufacturers of technology products and services.

Companies that do business with the United States government face increasingly strict data security requirements for how they manage, store and process sensitive government information, with mandatory reporting of data breaches and standards for safeguarding sensitive data. For example, the Cybersecurity EO includes updates to federal contracting language involving cybersecurity incident reporting, which may eventually be implemented through Federal Acquisition Regulatory Council rules. Under the Cybersecurity EO, the National Institute of Standards and Technology (NIST) also issued guidelines related to source code testing for software developers acting as government vendors. In May 2023, the NIST further updated its draft guidelines for protecting sensitive unclassified information (NIST Special Publication [SP] 800-171 Revision 3) to help organisations with implementation and address threats posed to controlled unclassified information. NIST anticipates one more draft version of 800-171 before its final version is published in early 2024.

At the same time, legislators at the state and federal level are exploring the creation of privacy rules that include mandatory data safeguarding requirements for personal information. There are now 10 US states with comprehensive privacy laws – Colorado, California, Virginia, Utah, Connecticut, Indiana, Tennessee, Texas, Montana and Iowa. This number is growing rapidly as many other states are exploring potential new laws. These state laws generally require that entities provide reasonable administrative, technical and physical security practices to protect personal information. Still, many of these state laws exempt companies that are governed by other federal laws, like the Gramm-Leach-Bliley Act (GLBA), a regulation applicable to financial service entities that was enacted in 1999. Perhaps because the GLBA has not been updated in more than two decades, in 2023 the House Financial Services Committee introduced the Data Privacy Act of 2023 to modernise the GLBA.

There also continues to be an interest in instituting a comprehensive federal data protection bill. Congress held multiple hearings in 2021 and early 2022 to investigate a perceived need to pass a comprehensive federal data protection law and in 2022, the American Data Privacy Protection Act (ADPPA) made history as the first such bill to make it out of committee. The Innovation, Data, and Commerce Subcommittee of the House Committee on Energy and Commerce continued this effort, holding a hearing on the ADPPA in March 2023.

We anticipate these trends will ultimately (although perhaps not expeditiously) lead to more uniform and clear cybersecurity standards, along with related privacy rules. In the meantime, federal agencies in the United States are likely to continue efforts to aggressively police cybersecurity regulatory compliance applicable to particular economic sectors and to seek to impose new requirements on companies responding to breaches.

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?

The United States does not have a uniform data breach notification law. Rather, all 50 states, as well as the District of Columbia and a number of territories, have individual data breach notification laws. At the federal level, sector-specific laws for government contractors, certain financial institutions and certain businesses handling health records also impose special breach notification rules. In general, data breaches mandate notification to regulators and consumers when specific categories of sensitive personally identifying information are compromised through a cyber intrusion, inadvertent disclosure or other loss of data. For example, in many jurisdictions, the unauthorised acquisition of or access to data that includes name combined with a social security number, financial account number, driver's licence number, health record or passport number would likely trigger a mandatory breach notification obligation to the consumer and may also trigger notification obligations to regulators. States are continuing to expand their definitions of covered information, with username or email address in combination with a password or security questions and answers as well as biometric data becoming subject to breach notification requirements. State regulators are also increasingly investigating cyber incidents and bringing enforcement claims for perceived lapses in reasonable cybersecurity controls.

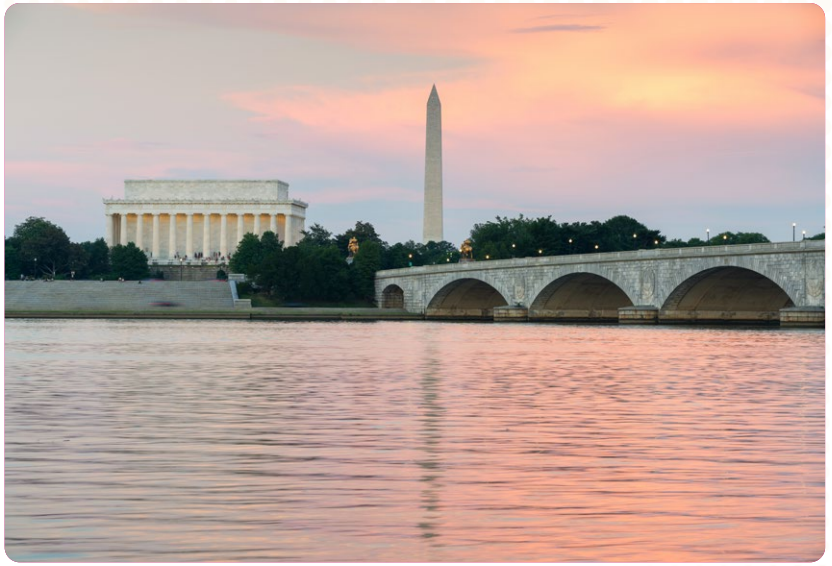


Photo by Romiana Lee on Shutterstock

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

Data security incidents, particularly cyber intrusions, may raise many significant challenges. For companies handling substantial amounts of sensitive personal information, such incidents may trigger:

- communications challenges for companies that want to provide consumers or other customers with reassurance while also investigating the scope of a particular incident;
- reputational and financial challenges as incidents can impact brand stability, stock price, and a company's relationship with customers and other third parties that do business with it;
- remediation challenges in taking steps to further safeguard sensitive data to both stop a cyber intrusion and to help bolster existing security;

"States are continuing to expand their definitions of covered information, with username or email address in combination with a password or security questions and answers as well as biometric data becoming subject to breach notification requirements."

- investigative challenges to determine the scope of the intrusion, what data was taken and whether the attacker has been removed from the company's networks; and
- protracted legal challenges as some incidents may trigger ongoing regulatory investigations and consumer class action litigation, which can require significant time and resources.

Managing these sorts of challenges, often while also coordinating with law enforcement authorities, regulators, stakeholders and affected individuals, requires all components of a business to work together. Such incidents are not just the province of the information technology team. They are, rather, problems that require senior, and where applicable, board-level attention to manage and address.

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

Incident response requires an immediate, coordinated effort to gather the facts through forensic analysis and to execute an incident response plan that enables the company to address multiple work streams simultaneously in a coordinated fashion. The response generally prioritises remediation, reputational harm, communication with all the relevant constituencies (including, critically, customers) and preparing for the range of potential regulatory inquiries and litigation.

Companies can take several steps to best prepare for and improve their ability to respond to such issues, including:

- reviewing existing incident response plans, benchmarking against industry best practices on a regular basis, and proposing changes. Plans should also be reviewed after any serious incident

Photo by Orhan Cam on Shutterstock

to incorporate lessons learned from the company's response to that incident;

- developing and participating in tabletop exercises to help those with implementation responsibilities understand how the incident response plan would work in practice;
- engaging third-party service providers and firms in advance, through counsel, to ensure that the right resources are available to address critical issues in a time-sensitive manner and under attorney–client privilege;
- conducting regular risk assessments of a company's information technology infrastructure, systems and controls to identify and mitigate risk to the extent that risk does not align with the entity's business goals. This may also include assessments of vendor cybersecurity given the risk of exploited supply chain vulnerabilities;
- providing regular updates on, and analysis of, legal and regulatory developments that would influence response plans and practices; and
- training employees, not just those involved in information security, to recognise potential security risks.

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

Cloud services trigger a variety of risks, similar to those faced in IT outsourcing, that should be carefully balanced as part of the decision to outsource data storage or other information technology functionality. Those risks include the following:

- third-party access to data. When company information is outsourced for storage or other processing by third parties, that information may no longer be solely within the control of the information owner. The cloud provider may be compelled to release it to third parties in litigation or to government agencies inside or outside the United States. Moreover, absent appropriate prohibitions in the parties' agreement, a cloud provider may be entitled to share customer data (or data derived from customer data) with third parties for the cloud provider's own business purposes;
- data security. Evaluating the security of data in a cloud environment and ensuring the use of appropriate safeguards can be very challenging. Many cloud providers will not provide full visibility into their own network security posture;
- location of data. Data entrusted to a third party may be stored or otherwise processed in a jurisdiction that gives rise to unique legal or regulatory concerns. Moreover, some cloud providers do not provide transparency or assurances concerning where the data will be located;
- privacy and consumer notice. Processing of consumer data by a third-party cloud provider may necessitate special notices to

"Other regulations are cloud-specific, such as ISO 27017, an independent security standard that provides guidance on the information security aspects of cloud computing and is often used by organisations to judge their ability to manage data in a cloud environment."

consumers or employees and it may trigger a number of privacy and data protection obligations with respect to how their data will be handled, retained and distributed; and

- business continuity or provider lock-in. Cloud providers and sub-processors may go out of business or otherwise experience a disaster or other incident that results in the loss, corruption or temporary inaccessibility of their customers' data. Further, it may be difficult to extricate data from a software as a service solution at the end of the parties' engagement, at least in a format that does not require substantial processing before the data can be ingested into a competitor's software as a service product.

There are a wide range of different regulatory regimes that impact cloud outsourcing. Some regulations that are agnostic about whether data is outsourced in a cloud environment or remains within a company's firewall, impose general obligations that have the effect of imposing rules that data owners must satisfy in a cloud scenario (such as National Institute of Standards and Technology requirements to track and specially secure sensitive data). Other regulations are cloud-specific, such as ISO 27017, an independent security standard that provides guidance on the information security aspects of cloud computing and is often used by organisations to judge their ability to manage data in a cloud environment. Certain sectors, particularly the financial services and government contracting sectors, are subject to more stringent requirements on their use of cloud services to host consumer or government data.

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

Cybersecurity remains a substantial focus of federal and state law enforcement efforts in the United States and is an area of particular concern as destructive ransomware events become more common

QUESTIONS

and more substantial. The Federal Bureau of Investigation has grown its cyber capabilities substantially over the past several years, and President Biden's administration is increasingly focused on efforts to combat ransomware groups.

Specific laws that address criminal activity in the cyber context include the Computer Fraud and Abuse Act, which outlaws intrusions into or interference with the security of a government computer network or other computers connected to the internet. In addition, several federal surveillance laws prohibit unauthorised eavesdropping on electronic communications, which can limit a variety of cybersecurity activities. For example, the Electronic Communications and Privacy Act prohibits unauthorised electronic eavesdropping. The Wiretap Act prevents the intentional interception, use or disclosure of wire, oral or electronic communication, unless an exception applies. The Stored Communications Act precludes intentionally accessing without authorisation a facility through which an electronic communication service is provided and thereby obtaining, altering or preventing authorised access to a wire or electronic communication while it is in electronic storage.

The Biden administration has made its focus on cybersecurity clear. In March 2023 it issued its new National Cybersecurity Strategy, outlining its approach to defending critical infrastructure, using market forces to encourage improved cybersecurity practices, and investing in cybersecurity moving forward.

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

Cybersecurity and privacy is often a core topic for M&A due diligence because of potential regulatory or litigation exposure that a company may take on through an acquisition. Acquirers often seek special assistance to evaluate the scope of exposure by examining the nature of the target business, the type of data it collects, maintains and shares about customers or third parties and the regulatory environment in which it operates. Acquirers may also evaluate the types of controls the company has in place to protect its systems, limit data sharing to permissible means and otherwise ensure compliance with regulatory requirements. After the transaction is complete, acquirers need to pay close attention to ensure that the target company is either fully integrated or that the target's privacy and data security practices are brought into line with the acquirer's risk tolerance.

Jason Chipman
jason.chipman@wilmerhale.com

Benjamin Powell
benjamin.powell@wilmerhale.com

Arianna Evers
arianna.evers@wilmerhale.com

Shannon Togawa Mercer
shannon.mercer@wilmerhale.com

WilmerHale
Washington, DC
www.wilmerhale.com

Read more from this firm on Lexology

QUESTIONS

The Inside Track

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

Legal advice around cybersecurity issues requires counsel who is experienced at addressing and managing the wide range of issues that cybersecurity incidents and related preparation activities may trigger.

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

Cybersecurity is an evolving and changing field that requires lawyers to provide a mix of legal, policy and business guidance to clients navigating new and often challenging issues. An increasingly large number of federal and state regulatory agencies, categories of litigation plaintiffs and business partners or customers are interested in understanding how companies are protecting their data, resulting in an increasingly complex web of risks.

How is the privacy landscape changing in your jurisdiction?

Privacy is becoming a critical part of contracting arrangements between parties, with greater focus on compliance with state, national and international laws. Greater regulation of the handling, securing and transfer of data is resulting in an increasing focus by companies on privacy issues, particularly on specifying the obligations that must be met in the handling of data between parties. The California Consumer Privacy Act of 2018 went into effect in 2020 and was amended by the California Privacy Rights Act on 1 January 2023, and new laws in California, Utah, Connecticut, Virginia, Colorado, Indiana, Tennessee, Texas, Montana and Iowa have either gone into effect or will go in to effect in the near term.

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

Understanding about cyberthreats is generally increasing in the United States. High-profile incidents involving espionage and criminal actors receive frequent public attention. But companies need to be constantly on guard for the latest threats. In the recent past, incidents involving tax fraud were on the rise and today ransom and extortion demands associated with cyber intrusions are common.

About Market Intelligence

Respected opinion, expert judgement

Lexology GTDT: Market Intelligence provides a unique perspective on evolving legal and regulatory landscapes in major jurisdictions around the world. Through engaging, easily comparable interviews, the series provides the legal profession's thought leaders with a platform for sharing their views on current market conditions and developments in the law.

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 interesting cases and deals.

Read more Market Intelligence topics