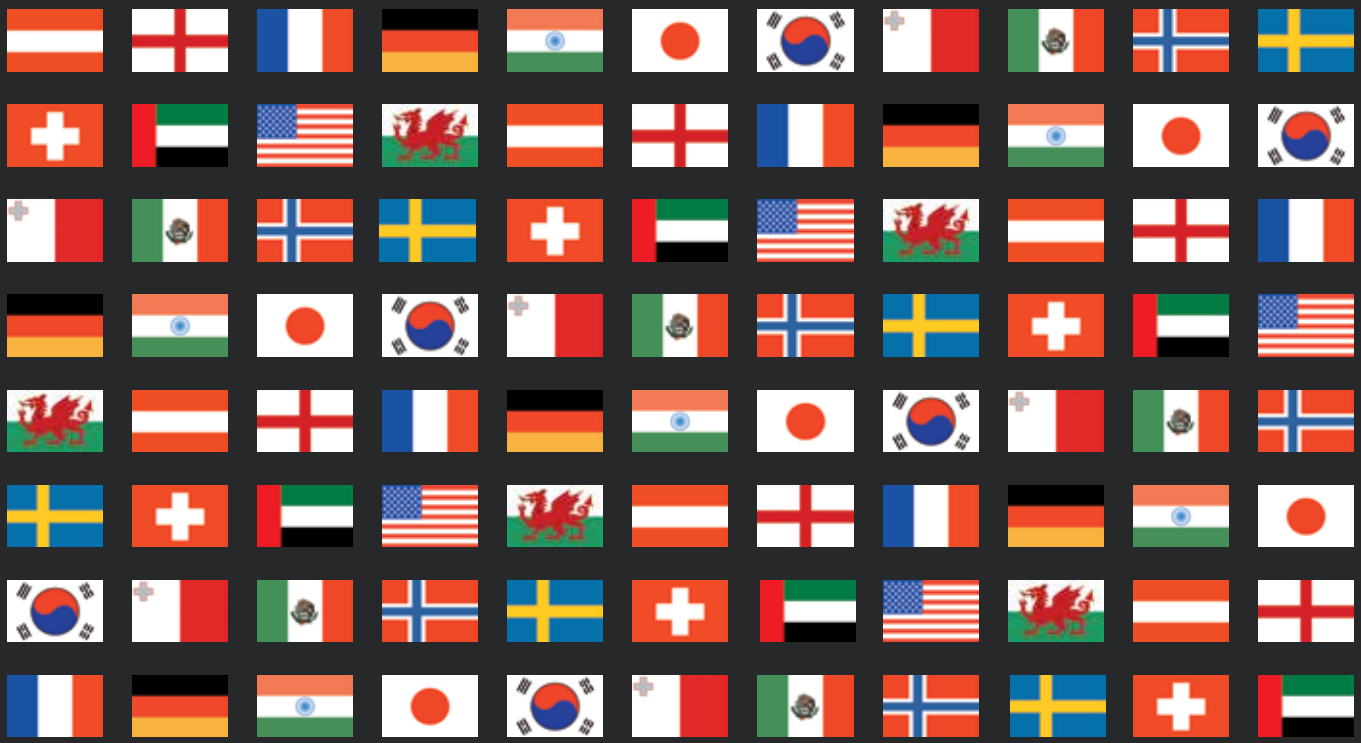
Cybersecurity

Contributing editors
Benjamin A Powell and Jason C Chipman



2016

GETTING THE DEAL THROUGH

GETTING THE DEAL THROUGH

Cybersecurity 2016

Contributing editors

Benjamin A Powell and Jason C Chipman

Wilmer Cutler Pickering Hale and Dorr LLP

Publisher
Gideon Roberton
gideon.roberton@lbresearch.com

Subscriptions
Sophie Pallier
subscriptions@gettingthedealthrough.com

Business development managers
Alan Lee
alan.lee@gettingthedealthrough.com

Adam Sargent
adam.sargent@gettingthedealthrough.com

Dan White
dan.white@gettingthedealthrough.com

Law Business Research

THE QUEEN'S AWARDS FOR ENTERPRISE: 2012

Published by
Law Business Research Ltd
87 Lancaster Road
London, W11 1QQ, UK
Tel: +44 20 3708 4199
Fax: +44 20 7229 6910

First published 2015
Second edition
ISSN 2056-7685

Printed and distributed by
Encompass Print Solutions
Tel: 0844 2480 112

CONTENTS

Preface

Cybersecurity 2016

Second edition

Getting the Deal Through is delighted to publish the second edition of *Cybersecurity*, which is available in print, as an e-book and online at www.gettingthedealthrough.com.

Getting the Deal Through provides international expert analysis in key areas of law, practice and regulation for corporate counsel, cross-border legal practitioners, and company directors and officers.

Throughout this edition, and following the unique **Getting the Deal Through** format, the same key questions are answered by leading practitioners in each of the jurisdictions featured. Our coverage this year includes chapters on Switzerland and the United Arab Emirates.

Getting the Deal Through titles are published annually in print. Please ensure you are referring to the latest edition or to the online version at www.gettingthedealthrough.com.

Every effort has been made to cover all matters of concern to readers. However, specific legal advice should always be sought from experienced local advisers.

Getting the Deal Through gratefully acknowledges the efforts of all the contributors to this volume, who were chosen for their recognised expertise. We also extend special thanks to the contributing editors, Benjamin A Powell and Jason C Chipman of Wilmer Cutler Pickering Hale and Dorr LLP, for their continued assistance with this volume.

GETTING THE DEAL THROUGH

London
January 2016

Global Overview

Benjamin A Powell, Jason C Chipman and Marik A String
Wilmer Cutler Pickering Hale and Dorr LLP

With interconnectivity and use of digital storage expanding, cyberthreats posed by nation states, commercial competitors, company insiders, transnational organised crime and 'hacktivists' are growing on a global basis. Recent high-profile data intrusions in the United States have brought particular attention to cyber espionage and cyber 'attacks' perpetuated by nation states, prompting data and information security to become a major geopolitical topic for relations between the United States and China, as well as several other nations. For commercial enterprises, cybersecurity is no longer a technical issue for information technology personnel; it is a high priority for corporate counsel, senior executives and company boards. In this environment, maintaining an effective corporate cybersecurity programme is likewise growing in importance.

The growth of cybersecurity as a distinct discipline is a result of the remarkable value of assets accessible within companies and across national borders in digitised formats. Organisations around the world regularly suffer data security incidents ranging from nuisance intrusions and petty theft to massive criminal conspiracies. The German government recently estimated that its companies lose between US$28 billion and US$71 billion (and 30,000 to 70,000 jobs) per year from economic espionage. Such data thefts are prompting more calls for reform and more emphasis on developing regulatory standards for minimal safeguards.

Some economic sectors are more vulnerable than others. In the past few years, global criminal networks have targeted personal and financial information of customers in the retail and financial services industries, foreign nations have stolen valuable intellectual property and anonymous hackers have sought to destroy or embarrass corporations and executives. Nevertheless, despite these real threats, a surprising number of companies lack formal information security policies and incident response plans. Critical infrastructure sectors have become a particularly common target for cyber intrusions: a 2014 survey by the Ponemon Institute of 599 executives from the power, oil, gas and water sectors in 14 countries found that 70 per cent of respondents had experienced network intrusions.

In response to these challenges, governments from around the world are implementing legal reforms and shifting enforcement priorities. In the European Union, the legal framework for cybersecurity among member states is evolving to deal with new threats. The European Commission has issued a Cybersecurity Strategy to bolster cyber resilience, develop a more coherent cyber defence policy and promote industrial cooperation. On 7 December 2015 the European Union agreed on the final text for a Network and Information Security Directive, which would improve cybersecurity cooperation and capabilities among member states and require operators of 'essential services' in certain sectors to take appropriate security measures. On 15 December 2015, the European Union reached an agreement on the final text for a new General Data Protection Regulation, which is likely to be approved by the European Parliament in early 2016. The Regulation will replace a 1995 Data Protection Directive that has been the basis for national data protection laws of EU member states. On 15 December 2015, the European Union also approved the final text of a new directive to protect against the theft of trade secrets and other confidential business information, which would introduce common definitions, provide more effective redress for theft and prioritise enforcement of such types of theft. In October 2015, the European Court of Justice issued a landmark decision that called into question the validity of US-EU 'safe harbour' arrangements, which had provided legal protections for companies that transferred personal data between the two jurisdictions. How this decision may impact the flow of data important for cybersecurity measures is not yet clear.

In the United States, dozens of federal and state statutes address cybersecurity issues, but no overarching statutory framework exists. The US Congress has considered several legislative proposals focused on enhancing critical infrastructure protection, bolstering information sharing, strengthening the protection of personal data and increasing criminal penalties for economic espionage and theft. A 2013 US Executive Order directed the development of a voluntary cybersecurity framework to incorporate industry best practices and called for an expansion of information sharing and collaboration between government and the private sector. US regulatory agencies are expanding enforcement actions to address cybersecurity issues. For example, the US Securities and Exchange Commission has issued guidance requiring companies to disclose material information on the nature of any cyberthreats and challenged numerous companies on the adequacy of their disclosures. Similar efforts to protect against cyber intrusions are taking place in other jurisdictions as well.

Following several high-profile cyber intrusion events in 2015, the United States has increased focus on international action to enhance cybersecurity and data protection. The US President issued an Executive Order authorising the imposition of economic sanctions against individuals or entities found to be engaged in malicious cyberactivity and agreed to a new cybersecurity framework with China intended to limit state-sponsored theft of corporate secrets. The Trans-Pacific Partnership trade agreement, which was recently agreed between the United States and 11 other nations also contains added protections for the theft of trade secrets and confidential information using computer systems.

Many reforms are also taking place within industry and are customer-driven. Payment card companies in the US are now requiring chips to tokenise payment card data. In a relatively new development for many companies, commercial customers around the world are increasingly adding cybersecurity requirements to contracts and demand controls on how information technology suppliers hold data in cloud centres or otherwise demand special obligations related to protecting data. Cybersecurity provisions are frequently a key part of negotiations involving outsourcing of data and the sharing of data between companies. In addition, companies may require audits and other rights and remedies to address cybersecurity challenges.

Around the globe, the cybersecurity legal landscape continues to rapidly shift as governments consider new laws, regulations and enforcement policies. In the years ahead, companies will be faced with an increasingly complex array of cybersecurity compliance challenges and risks. At the same time, governments are working to determine the appropriate regulatory policy to govern the rapidly changing information technology environment and the best framework for working with the private sector to improve the security of digital assets.

Austria

Árpád Geréd
Maybach Görg Lenneis & Partner

Legal framework

1 Summarise the main statutes and regulations that promote cybersecurity. Does your jurisdiction have dedicated cybersecurity laws?

Even though cybersecurity and, as a related topic, cybercrime, have a long history in Austrian rules of law, efforts to establish dedicated and detailed rules on cybersecurity that are binding not only for governmental agencies and (partially) state-owned companies but also the private sector are fairly recent.

The first legal provision on cybersecurity in its widest sense was article 10 of the then new Austrian Data Protection Act (DSG 1978), which entered into force in 1980. In this provision, data processors were obliged to set up work rules regarding data security, such as measures for access security or software testing. While the provision did not contain any details on the required rules and, further, took economic and technical feasibility into account, it required these internal rules to be approved by the Austrian Data Protection Commission (now the Data Protection Authority, or DSB), thus granting at least a minimum level of homogeneity.

In hindsight, article 10, despite its lack of detail, provided a solid basis for a unified understanding of required data security measures. But in 1987 this provision was amended with far-reaching consequences: first, the new article 10 no longer required data security measures to be compiled in a set of work rules; and second, the requirement for approval by the now DSB was removed. However, the modified provision still took into account the economic and technical feasibility of the measures as well as their adequacy related to the processed data.

In a country such as Austria, which is dominated by small and medium-sized enterprises, the flexibility of article 10 DSG 1978 coupled with a legal as well as factual lack of any control of the security measures taken led to a fragmentation of the level of cybersecurity and in extreme cases this led to very small enterprises not taking any relevant security measures at all, arguing that those were neither economically feasible, nor required by the type of processed data. Unfortunately this relatively toothless rule has found its way into article 14 of the current Austrian Data Protection Act (DSG 2000) in mostly unmodified form. While article 14 DSG 2000 applies to data controllers and data processors alike and corresponds in essence to article 17 of the Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, the EU Data Protection Directive, it is, nevertheless, a step backward from its predecessor, article 10 DSG 1978.

The first cybercrime-related rules were established in 1987 with articles 126a and 148a of the Austrian Criminal Code (StGB). These provisions penalised the damaging of data and the abuse of automated data processing (including the modification of processed data as well as the processing software) respectively. Depending on the damage caused, these actions were punishable by imprisonment of up to five or 10 years respectively.

In 2002 Austria adopted the Council of Europe's Convention on Cybercrime, modifying the StGB to also penalise acts such as the illegitimate access to a computer system (article 118a) or the abusive interception of data (article 119a).

With these provisions of the DSG 2000 and the StGB, a first basic set of cybersecurity rules was in place, obliging enterprises to take protective measures while at the same time protecting their efforts and systems by means of the Criminal Code.

While it was not until 2014 that new legal rules on cybersecurity were announced, Austrian private entities as well as the federal government were far from inactive in the meantime.

The first industry-wide initiative to centrally collect and manage cybersecurity incidents from the private as well as the public sector was the Computer Incident Response Coordination Austria (CIRCA), established by the Internet Service Providers Association (ISPA) in cooperation with the Austrian Federal Chancellery. In 2008 CIRCA was incorporated into the newly created Austrian Computer Emergence Response Team (CERT) as well as the Austrian Government Computer Emergency Response Team (GovCERT) with the former being primarily operated by the NIC.at, the Austrian domain registry, and the latter by the Federal Chancellery. Though factually important and well recognised, the main purpose of both CERT institutions lies in the collection of information on incidents and the coordination of the incident response. As such, both institutions may only advise on prevention measures but have no authority to demand certain actions.

Apart from these two most important CERTs, there are others established at authorities or formerly state-owned enterprises, such as the City of Vienna, A1 (the former state-owned telephone operator) or the Austrian Federal Computing Centre (BRZ), which is the former federal data centre and now e-government partner of the federal administration in Austria. These are all organised in the Austrian CERT-network (CERT-Verbund), which was established in 2011.

The most recent addition to the Austrian organisations active in the field of cybercrime is the Cyber Crime Competence Centre (C4), which was established in 2012. In contrast to the CERTs, the C4's aim is to actively combat cybercrime. Therefore, its personnel consists of members of the Austrian Federal Police as well as the Austrian Federal Ministry for Internal Affairs.

In May 2014 the Austrian government announced the introduction of a dedicated Austrian Cybersecurity Act. This announcement came in the wake of similar efforts in Europe, most notably the presentation of the draft version of a Network- and Information Security Directive by the European Commission in February 2012 and of a German law on cybersecurity, the IT Security Act, in March 2013. While the Austrian government originally announced that the new Cybersecurity Act should enter into force in early Autumn 2016, as yet, no draft has been published.

2 Which sectors of the economy are most affected by cybersecurity laws and regulations in your jurisdiction?

According to the official communications of the Austrian government, the envisioned Cybersecurity Act should ultimately regulate a broad selection of public as well as private entities. However, at first the focus should lie on public authorities including courts and private providers of critical infrastructure, in particular, finance, communication, energy and transportation.

The Austrian communication industry, including internet service providers, already has a headstart in the field of cybersecurity. This is not only due to IT forming the core or at least a substantial part of its business, but also due to the involvement of the Austrian communication industry in the CIRCA and now CERT. The same applies to a few public authorities, most notably the Austrian Federal Chancellery and the BRZ. These entities are also the ones to have made the most progress towards promoting cybersecurity.

Other industries, however, still need to improve to varying degrees. For instance, the financial sector in Austria features some leading but also unfortunately some less stellar examples. The Austrian energy sector has in the past mostly focused on downplaying the potential risks of networked power grids and smart metering in the media. The transportation sector also appears unevenly prepared to face cybersecurity challenges, with, for example, the Austrian Federal Railway (ÖBB) being one of the positive examples.

In 2014, the initiative Trust in Cloud (www.trustincloud.org) was launched by the EuroCloud.Austria, the Austrian association of the EuroCloud Europe, an independent non-profit organisation. Participants include national and international enterprises from the IT sector, but also public and private entities from other sectors, such as the Austrian Federal Chancellery, the ÖBB, an international supermarket chain and an international producer of skiing equipment. While the aim of the initiative is to promote cloud computing in general, cybersecurity is one of the major focus points.

3 Has your jurisdiction adopted any international standards related to cybersecurity?

Austria, more specifically the Austrian Standards Institute (ASI), which is the Austrian member of the European Committee for Standardization and the International Organization for Standardization has adopted all relevant international standards related to cybersecurity, most notably ISO/IEC 27001:2013 (currently ÖNORM ISO/IEC 27001:2015 09 01 in Austria).

4 What are the obligations of responsible personnel and directors to keep informed about the adequacy of the organisation's protection of networks and data, and how may they be held responsible for inadequate cybersecurity?

While Austrian law knows the concept of responsible persons (ie, employees responsible for certain areas of business within their company) this concept does not extend to cybersecurity or (unlike, for example, Germany) even data protection. Thus, (managerial) employees or directors in Austrian are liable only according to the general legal rules, which basically means that they need to act with due diligence and with the care of a prudent businessperson, as set forth by Austrian law and further detailed by rulings of Austrian courts.

While the DSG 2000 does require proportionate and adequate data security measures, consequences of default are generally borne by the company rather than any internally responsible employee or the director.

5 How does your jurisdiction define cybersecurity and cybercrime?

Austrian law knows no definition of either cybersecurity or cybercrime. While article 14 DSG 2000 does stipulate data security measures, it does not define data security, much less cybersecurity. Also the StGB penalises and defines certain acts of cybercrime, though it lacks a general definition of cybercrime as a whole.

In any case, cybersecurity in Austria is distinct from data privacy. Even though neither term is defined in Austrian law, from the DSG 2000 it becomes apparent that data privacy, in the Austrian understanding, primarily deals with the rights and obligations related to the usage of data obtained legitimately while the aim of data security, as an aspect of cybersecurity, is to prevent illegitimate access to and (ab)use of data.

6 What are the minimum protective measures that organisations must implement to protect data and information technology systems from cyberthreats?

Article 14 DSG 2000 requires any controller or processor of personal data to implement measures to ensure data security. However, such measures need to take into account the type, extent and purpose of the processed data, the state of the art and the economic feasibility.

Therefore, even though this provision does stipulate minimum protective measures, it is not clear what the minimum requirements in each case may be. Further, this provision only applies to personal data rather than any type of data.

As a result, in the field of cybersecurity industry standards and the recommendations of the CERT and GovCERT are more important in Austria than legal rules. This is especially true for relatively new technology such as cloud computing or the issues associated with various forms of bring your own device.

7 Does your jurisdiction have any laws or regulations that specifically address cyberthreats to intellectual property?

Article 40e and 40f of the Austrian Intellectual Property Act stipulate rules on decompilation of software and the use of databases respectively. While these rules do not address cyberthreats specifically, they are the only ones addressing this subject explicitly within the context of intellectual property.

Where cyberthreats to intellectual property involve acts of cybercrime, the rules of the StGB apply.

8 Does your jurisdiction have any laws or regulations that specifically address cyberthreats to critical infrastructure or specific sectors?

Currently, no Austrian laws exist specifically addressing cyberthreats to critical infrastructure. However, it is expected that the planned Cybersecurity Act will introduce such rules.

9 Does your jurisdiction have any cybersecurity laws or regulations that specifically restrict sharing of cyberthreat information?

Austria does not have any laws that would serve to restrict the divulging or sharing of information related to cyberthreats or cybersecurity incidents. On the contrary, the upcoming Austrian Cybersecurity Act is planned to oblige affected companies or institutions to report not only cybersecurity breaches, but also incidents, such as unsuccessful breaching attempts or activities that might indicate an impending attack. For this purpose, the Austrian Cybersecurity Act will most probably further require companies or institutions to whom it applies to set up an effective cyber risk management system.

10 What are the principal cyberactivities that are criminalised by the law of your jurisdiction?

The principal acts of cybercrime, relevant to businesses, which are penalised by the StGB depending on the amount of damage caused, are:

- illegitimate access to a computer system (article 118a);
- breach of telecommunication secrecy (article 119 StGB);
- abusive interception of data (article 119a StGB);
- abuse of audio recording or listening devices (article 120 para 2a);
- damaging of data (article 126a);
- disruption of the functionality of a computer system (article 126b);
- abuse of software or access data (article 126c);
- fraudulent abuse of data processing (article 148a); and
- forgery of data (article 225a StGB).

The fines are determined by the income of the culprit. Therefore, neither a minimum nor a maximum amount is stipulated by Austrian law.

11 How has your jurisdiction addressed information security challenges associated with cloud computing?

For the time being, the Austrian government, on the one hand, has not specifically addressed any of the challenges associated with cloud computing. On the other hand, private and non-profit organisations, such as the EuroCloud.Austria or the Austrian Chamber of Commerce, have made significant efforts to educate providers and especially (private and business) users of cloud computing solutions, be it by means of events or publications, such as White Papers and even a recommendation catalogue relating to cloud contracts (some of these publications are available in English and can be obtained from the website of the EuroCloud.Austria (www.eurocloud.at)).

Currently, the most important Austrian initiative regarding cloud computing is Trust in Cloud (www.trustincloud.org), which has formulated recommendations to the Austrian government, among others, in the field of cybersecurity. As the Austrian Federal Chancellery takes part in this initiative, it is realistic that those recommendations will be taken into account in the future.

Whether and to what extent cloud computing will be addressed in the planned Cybersecurity Act remains to be seen. However, since providers of cloud computing services are explicitly mentioned in the draft of the EU Network and Information Security Directive, it cannot be ruled out that they may also be subject to the Austrian Cybersecurity Act.

12 How do your jurisdiction's cybersecurity laws affect foreign organisations doing business in your jurisdiction? Are the regulatory obligations the same for foreign organisations?

As a draft of the announced Cybersecurity Act has yet to be published, it cannot be said with certainty whether and to what extent foreign organisations doing business in Austria will be affected by the Cybersecurity Act.

If the principles were based upon those of the DSG 2000, the rules would only apply to data used in Austria rather than any data from Austria. As an example, a foreign cloud provider would generally only need to obey the rules stipulated by its own jurisdiction. A user of the cloud services offered by the same provider, who employs those services in Austria, would, however, need to comply with Austrian cybersecurity rules. As a result, he or she would need to ascertain that the foreign cloud provider does the same.

Regarding data protection rules, this poses few problems in practice, as long as both the provider and the user are situated within the European Union. It, therefore, remains to be seen whether the cybersecurity rules (should they follow this system) would lead to the same result. As far as those rules will be based on industry standards, they should not pose problems even to providers from outside the European Union.

In any case, the rules of the European Union regarding the free movement of goods and services will need to be observed.

Best practice

13 Do the authorities recommend additional cybersecurity protections beyond what is mandated by law?

As there are currently no substantial laws on cybersecurity in Austria, enterprises need to rely on industry standards and recommendations by various organisations and authorities.

The first contact in the field of cybersecurity in Austria is the CERT for private entities and the GovCERT for the public sector. Both institutions not only coordinate responses to cyberthreats but also advise on prevention measures. Thus, they constitute the most important contributors to a harmonised understanding of required and recommended cybersecurity measures.

Further, interested parties can find a multitude of freely available publications on this topic, for example, from the Federal Ministry for Internal Affairs, the Chamber of Commerce or associations specialised on IT topics.

It remains to be seen whether or how far the relevancy of these institutions and their recommendations will be affected by the planned Cybersecurity Act.

14 How does the government incentivise organisations to improve their cybersecurity?

While the Austrian government is very active in promoting cybersecurity directly as well as indirectly (eg, by means of the GovCERT), there are currently no incentives in this context.

Judging from the discussions on the Cybersecurity Act it is currently expected that the Act will not change this situation but rather follow the 'classical' approach and penalise inadequate cybersecurity measures.

15 Identify and outline the main industry standards and codes of practice promoting cybersecurity. Where can these be accessed?

In Austria, ÖNORM ISO/IEC 27001:2015 09 01 (which can be obtained from the ASI against payment) as well as the recommendations of the CERT (available from their homepage: www.cert.at) can be regarded as the main industry standards and codes of practice in the field of cybersecurity.

Comprehensive guidelines summarising the relevant rules and recommendations as well as a checklist created specifically for very small enterprises have been created by the Austrian Chamber of Commerce and can be obtained from the microsite www.it-safe.at.

16 Are there generally recommended best practices and procedures for responding to breaches?

Best practices and procedures can be derived from industry standards or recommendations of the CERT. They may vary depending on the type, severity and potential danger of a breach. Thus, no general rules apart from containing the breach and saving any information for later analysis.

After the incident it is considered best practice to have the existing data analysed by a trustworthy, independent third party to determine the methods and reasons for which the system could be breached and to take measures to prevent such occurrences in the future.

17 Describe practices and procedures for voluntary sharing of information about cyberthreats in your jurisdiction. Are there any legal or policy incentives?

Voluntary information on cyberthreats should be addressed to the CERT (or the GovCERT, in the case of a public entity) by means of an e-mail containing:

- where the incident has occurred (eg, IP address, website);
- the nature of the incident (eg, a virus, a DoS attack);
- how the incident has been noticed (eg, log files);
- a request for feedback; and
- an electronic signature.

As there are no recommended standard procedures the notifying entity can follow in the meantime, it will need to wait for a response from the CERT. In any case, records of the incident should be saved in case they are destroyed or modified during the incident.

Unfortunately, currently, there are no incentives to voluntarily disclose information on cyberthreats apart from peer pressure within the industry.

18 How do the government and private sector cooperate to develop cybersecurity standards and procedures?

In the field of cybersecurity, cooperation between the private and the public sector has a long tradition in Austria, its first highly visible project being the CIRCA, established in 2003 by the ISPA and the Federal Chancellery.

Nowadays, the cooperation continues mainly within the Austrian CERT network, where the most important stakeholders from the private as well as the public sector are united either directly or indirectly through the participating CERTs. Within this network not only is the collected information on incidents or threats exchanged but the incident response and the advice on prevention measures are also coordinated.

The results are then propagated by the participants to other organisations, such as the Chamber of Commerce, which issue recommendations to their members, usually in the form of publications. Of course the flow of information works both ways.

In December 2014, Curatorship Safe Austria, an independent association focused on issues related to internal security, organised a large scale cybersecurity exercise focused on threats to critical infrastructures, in which, among others, the CERTs, the Federal Ministry for Internal Affairs and various private enterprises participated. The aim of the exercise was to optimise communication between the participants, especially the stakeholders as well as the organisations serving as information hubs for their respective sectors. Smaller exercises were conducted in 2015 and the results and experience gained during those exercises are planned to be taken into consideration for the upcoming Cybersecurity Act.

19 Is insurance for cybersecurity breaches available in the jurisdiction and is such insurance common?

Insurance against cybersecurity incidents, covering the costs of, for example, data recovery or downtime, are offered by every major insurer active in Austria. In detail, the covered risks of course vary from offer to offer with some covering even in the case of negligence or fault.

Despite the availability, cybersecurity insurance is as yet far from common. It remains to be seen whether this will change upon the introduction of the Cybersecurity Act.

Enforcement

20 Which regulatory authorities are primarily responsible for enforcing cybersecurity rules?

In Austria, due to a lack of regulatory rules regarding cybersecurity, no authority exists that is primarily responsible for enforcing cybersecurity rules. The only authority that may, among others and to a very small extent, enforce data security rules and penalise non-compliance is the DSB.

According to article 52, paragraph 2, subparagraph 2 DSG 2000, the DSB may impose a fine of up to €10,000 on any business that has, through gross negligence, failed to implement the data security measures set forth in article 14 DSG 2000. Thus, the powers of the DSB are very limited as far as cybersecurity is concerned.

The prosecution of cybercrime is handled by the C4, which acts as a special unit of the Austrian Federal Police or the Austrian Federal Ministry

for Internal Affairs, as the case may be. Therefore, the powers of the C4 equal those of the authority they represent.

It should be noted that breaches of the DSG 2000, thus, also a breach of the provision on data security measures, constitute an act of unfair competition under Austrian law. As a consequence, enterprises may call upon the courts if they accuse a competitor of breaching data privacy or data security provisions. In practice, this poses the most relevant risk of litigation in the context of the DSG 2000.

21 Describe the authorities' powers to monitor compliance, conduct investigations and prosecute infringements.

In the case of an alleged breach of data security provisions, the DSB initiates formal proceedings in which it can request statements and documents from any company concerned. Should the company fail to comply with this request, the DSB, similar to Austrian courts, is entitled to base its decision on the facts at hand but it cannot force the company to disclose any information.

The C4, on the other hand, has access to all measures available to the Austrian Federal Police or the Austrian Federal Ministry for Internal Affairs. Thus, they are, for instance, even able to have documents confiscated. Since they are limited to the prosecution of cybercrime, however, they may not use their powers to merely monitor compliance with or prosecute infringements of data security rules.

22 What are the most common enforcement issues and how have regulators and the private sector addressed them?

Due to the state of cybersecurity rules in Austria, no enforcement actions have been brought against the concerned companies by the Austrian authorities. In the publicly known cybercrime cases, especially attacks by the hacktivist group Anonymous, Austrian police have prosecuted the participating persons with varying degrees of success. However, no enforcement measures have been taken against the companies and institutions whose IT systems have been breached. Rather, they have received support by cybersecurity organisations to better secure their systems for the future.

23 What penalties may be imposed for failure to comply with regulations aimed at preventing cybersecurity breaches?

Apart from court actions by competitors, the only possible penalty under Austrian law is a fine of up to €10,000, which may be imposed by the DSB.

See question 20 for details.

24 What penalties may be imposed for failure to comply with the rules on reporting threats and breaches?

The only data breach provision in Austrian law is article 24, paragraph 2a DSG 2000, stipulating that if a data controller learns that personal data from his or her data application are systematically and seriously misused and the data subject may suffer damage, he or she shall immediately inform the data subject in an appropriate manner. However, such obligation to notify does not exist if the information – taking into consideration that only minor damage to the data subject is likely and the cost of the information to all persons concerned – would require an inappropriate effort.

Update and trends

Cybersecurity continues to be a hot topic in Austria as more and more industries become aware of how much they depend on information technology and that, essentially, any IT system may become the aim of a cyberattack. This is especially true for the much hyped Industry 4.0, which has by now also found its way into the current programme of the Austrian government. As a result, cybersecurity is now increasingly becoming a topic in IT contract negotiations and business customers more often than before require their business partners to consult independent forensic firms after a breach of or attack to their systems has become known.

The most relevant new development will be the introduction of a dedicated Austrian Cybersecurity Act, probably in autumn 2016. The extent to which this law will change the current cybersecurity environment cannot yet be determined. However, it is expected that notification requirements will be introduced regarding cyberthreats and cybersecurity incidents, independent of whether personal data is concerned or not.

This provision has unfortunately been heavily diluted in the political discussion process and is generally considered vague to the point of incomprehensibility. Especially the criteria of 'systematical and serious misuse', information of the data subjects 'in an appropriate manner', coupled with the possibility to take into consideration the 'cost of the information' and whether 'only minor damage' is likely, provide concerned enterprises with a very broad range of options, including not to notify at all.

In the unlikely event that a breach of the notification requirement is, nevertheless, clear, the DSB may impose a fine of up to €10,000.

This provision, further, only applies to breaches where personal data is affected. As a result, no notification requirement exists for cyberthreats or breaches where no personal data is involved (though the latter is statistically quite unlikely).

That said, it is expected that the planned Cybersecurity Act will introduce data breach notification requirements that will go well beyond the scope of article 14 DSG 2000. Details, however, are as yet unknown.

25 How can parties seek private redress for unauthorised cyberactivity or failure to adequately protect systems and data?

Due to the lack of any specific rules on cybersecurity and the consequences of non-compliance, in Austria private redress can only be sought before civil courts following general tort rules. This means that any person seeking redress would need to claim a concrete amount for damages and also prove that the damages in the desired amount have actually been caused by the defendant.

Even in the case of a breach of article 14 DSG 2000, parties would need to call upon civil courts for any redress as the DSB may only impose fines. Nevertheless, the decision of the DSB would be required in such a case to determine whether a breach of article 14 DSG 2000 has occurred in the first place.

MAYBACH · GÖRG · LENNEIS
& PARTNER RECHTSANWÄLTE

Árpád Geréd **a.gered@mglp.eu**

Museumstrasse 5
1070 Vienna
Austria

Tel: +43 1 997 19 66
Fax: +43 1 997 19 66 100
www.mglp.eu

Threat detection and reporting

26 What policies or procedures must organisations have in place to protect data or information technology systems from cyberthreats?

Apart from industry standards and recommendations, the only Austrian legal rule is that of article 14 DSG 2000.

See question 6 for details.

27 Describe any rules requiring organisations to keep records of cyberthreats or attacks.

As such records do not fall within the scope of Austrian legal rules on the keeping of documents (eg, contracts, invoices), the only applicable 'rules' are those determined by industry standards or recommendations.

See question 15 for details.

28 Describe any rules requiring organisations to report cybersecurity breaches to regulatory authorities.

Once again, apart from industry standards and recommendations, the only relevant Austrian legal rule in this regard is that of article 14 DSG 2000. It should be noted that this provision does not require the processor to notify the authority but rather the concerned data subjects.

See question 24 for details.

29 What is the timeline for reporting to the authorities?

Article 14 DSG 2000 requires data subjects to be notified 'without delay'. However, this provision does not require the notification of any authority.

See question 24 for details.

30 Describe any rules requiring organisations to report threats or breaches to others in the industry, to customers or to the general public.

Austrian legal rules neither require the reporting of cyberthreats, nor do they require reports to be issued to others in the industry or the general public.

See question 24 for details.

England & Wales

Michael Drury
BCL Burton Copeland

Legal framework

1 Summarise the main statutes and regulations that promote cybersecurity. Does your jurisdiction have dedicated cybersecurity laws?

There is no dedicated cybersecurity law as such in England and Wales. Rather, there are numerous statute-based laws, underpinned by the common law. These:

- criminalise interference with computers without authority, including where the intention is to commit other crimes by means of accessing computers, altering computer programs or producing 'hacking tools', or where the result is one of serious damage to the economy, environment, national security or human welfare, or significant risk thereof (the Computer Misuse Act 1990 (CMA) as amended by the Serious Crime Act 2015 (SCA));
- criminalise the interception of communications, which includes communications sent or received by computers (the Regulation of Investigatory Powers Act 2000 Part 1 (RIPA));
- impose obligations to protect personal data (rather than data more generally) by the application of security measures (by the Data Protection Act 1998 (DPA), especially within Schedule 1). The Seven Data Protection Principles are that the data is used fairly and lawfully; used for limited, specifically stated purposes; used in a way that is adequate, relevant and not excessive; accurate; kept for no longer than is absolutely necessary; handled according to people's data protection rights; and kept safe and secure. A breach of the obligation to keep data secure gives rise to potential criminal sanction, and civil financial penalties can be imposed on the data controller by the Information Commissioner, the UK public official responsible for policing the protection of personal data. Civil remedies are also available to data subjects where there has been a breach of the requirements of the DPA, including where processing by the person controlling the personal data is done in a manner causing, or likely to cause, substantial damage to the data subject;
- criminalise actions amounting to fraud (Fraud Act 2006 (FA)) and infringing intellectual property rights (Copyright, Designs and Patents Act 1988); and
- give rise to actions under the common law, in particular, the tort of negligence, where, if insufficient steps are taken to protect data or information held electronically, the person responsible for loss of the data could be held liable in civil law.

It is important to note that there will be significant changes to be brought about by the implementation of the General Data Protection Regulation and the Network and Information Security Directive agreed by the EU institutions in December 2015 (see question 3 and 'Update and trends').

Aside from emphasising in policy the benefits of good cybersecurity, English law, therefore, predominantly seeks to encourage cybersecurity by punishing breaches (notably in failures by those who are 'data controllers' of others' personal data to keep personal data secure) rather than by reward.

What would otherwise be breaches of law as above are made lawful where conducted by state agencies (principally) in the interests of national security and for the prevention and detection of serious crime, and in accordance with the authorisation regimes established under RIPA, the Police Act 1997, and the Intelligence Services Act 1994.

Parliament has not legislated to promote cybersecurity as such, and the offences described have been created in a rather piecemeal approach. The UK government has instead approached the cybersecurity issue by seeking to develop awareness, both in the business sector and among the public more generally, to enhance cybersecurity safeguards against, and mitigate the risks of, cyberattacks.

The CMA, which stands as the principal statute implementing the Budapest Convention on Cybercrime, provides for criminal offences based on the notion that if a person causes a (i) computer to perform any function with intent to secure access to any program or data held in any computer or to enable any such access to be secured; (ii) the access he or she intends to secure or to enable to be secured is unauthorised; and (iii) he or she knows at the time when he or she causes the computer to perform the function that this is the case, he or she is guilty of an offence. Such offences are punishable by imprisonment, some carrying a maximum sentence of life imprisonment where the attack causes or creates a significant risk of serious damage to human welfare or national security.

Securing access to a computer or a program encompasses many different actions. 'Computer' is not defined in the CMA. Access is said to be unauthorised if not done by a person who has responsibility for the computer and is entitled to determine whether the act may be done, or is done without the consent of such a person. What constitutes consent in the cyber world may be open to argument, but the courts are anxious to limit what might be so regarded. For example, the English Court of Appeal has determined that a distributed denial of service (DDoS) attack constitutes an action done without consent despite the suggestion that a computer is designed to receive communications.

The CMA creates further offences where the unauthorised access is sought with a view to committing other offences, for example, theft or fraud, or to impair the operation of a computer, which would include the implanting of viruses or spyware and DDoS attacks. In such cases, penalties are higher, in the latter case of up to 10 years' imprisonment. The CMA also criminalises the making, adapting, supplying or offering of articles to be used in committing the CMA offences of unauthorised access, etc.

The DPA, which implements the EU Data Protection Directive (95/46/EC), requires data controllers to meet the following standard as far as data security is concerned: '[a]ppropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data' (Seventh Data Protection Principle, Schedule 1 DPA). In essence, an organisation must take steps to prevent unauthorised access, and accidental loss or damage. Failure to meet these standards can lead to a civil penalty or a criminal sanction (sections 55A and 55 DPA respectively).

Other criminal offences are dealt with under the relevant questions below.

2 Which sectors of the economy are most affected by cybersecurity laws and regulations in your jurisdiction?

Cybersecurity laws and regulations affect all businesses and organisations that process and control data. The DPA applies specifically to personal data, namely, data from which a living person can be identified. As such, cybersecurity laws and regulations affect all sectors of the economy.

Presently, there are no specific sectoral laws (except, to some extent, for the providers of public communications services (see question 3)), but businesses of any size will have to meet the DPA requirements to the extent that they will be processing personal data (and virtually all will do

so). Government guidance and publicity was traditionally directed towards the defence sector but is now addressed to all businesses and sectors due to the pervasive nature of the threats and breaches. Guidance, which is extensive and frequently published, and compliance standards tend to be structured around the types of attacks, rather than the industries attacked. There are some examples of sectoral guidance, for example, the Payment Card Industry Data Security Standard (PCI DSS) must be complied with by all organisations that accept, store, transmit or process cardholder data, to decrease payment card fraud. There is no data to suggest that any sector is doing much better than any other. The finance sector, where there is an obvious risk of fraud, may be thought to have considered these matters for longer, and in greater depth, than others. However, the increasing prevalence of threats and breaches is evident from data that shows that 90 per cent of large businesses and 74 per cent of small businesses have had a security breach in 2015, up from the already high 81 per cent for large businesses and 60 per cent for small businesses in 2014.

Professional regulators are increasingly engaged in the participation of cybersecurity initiatives, at times embedding national strategies and guidance into their own regulatory guidance. The Solicitors Regulatory Authority, for example, has encouraged the use of the government's '10 Steps to Cyber Security'.

Failure to adequately protect data may give rise to breaches of regulatory requirements more generally. For example, the Financial Conduct Authority (FCA) has levied penalties for data breaches where they have been found to constitute breaches of FCA Principle 3 to 'take reasonable care to organise and control its affairs responsibly and effectively, with adequate risk management systems' by failing to take reasonable care to establish and maintain systems and controls appropriate to the business, or to counter the risk that a business might be used to further financial crime.

3 Has your jurisdiction adopted any international standards related to cybersecurity?

The European Union has and continues to have a key role in setting standards for the United Kingdom.

First, Directive 95/46/EC was designed to protect the privacy of all personal data collected for or about citizens of the EU. This has been given effect in England and Wales by the DPA and affects any organisation that collects or processes personal data (see question 1).

Second, Directive 2013/40/EU on attacks against information systems aimed to create a unified approach to the types of and punishments for cyber offences through the EU. The Directive was given effect in the UK by the Serious Crime Act 2015 (SCA), which amended the CMA to include new and extend existing offences, and to increase the maximum penalty for some cyber offences to life imprisonment.

Most recently, the EU has been promoting the European Commission's Cyber Security Strategy of 2013. Of the greatest significance, on 15 December 2015, the EU Parliament, Council and Commission agreed the text of the long-anticipated General Data Protection Regulation. On 7 December 2015, the same three EU institutions had agreed the Network and Information Security Directive, the first EU wide legislation on cybersecurity in a directive with measures to ensure a high common level of network and information security. In addition, a third measure, a directive concerning data protection in the field of law enforcement, which seeks to maintain the protection of individuals where their data is processed for prevention, detection, investigation and prosecution of crime or to safeguard against and prevent threats to public security has also been agreed by the institutions.

This legislation is the most prescriptive of its kind, and will generally apply to all data controllers and processors established in the EU and processing personal data of subjects who are in the EU. Several key provisions of the Regulation should be noted in the cybersecurity context. The first is a uniform requirement for notification of security breaches. The effects of the requirement of telecommunications providers to notify the supervisory authority of any actual breaches without undue delay under EU Regulation 2013/611/EU will apply under the new Regulation, albeit to a much wider range of organisations. In addition, there is also a requirement to notify the affected data subjects if the breach is likely to result in a high risk to the rights and freedoms of individuals, unless the organisation had applied appropriate security measures either before or after the breach to effectively counteract this high risk. Second, the Regulation affects both data controllers and data processors. In relation to the latter, it now sets out clear obligations which include the responsibility to implement technical and organisational security measures, appropriate to the specific risks that are present. It also includes the requirement to assist data controllers in any data subject access requests, thus facilitating individuals' access to their personal data. The Regulation further sets out clear provisions for the transfer of data, which is possible with adequate consent, when based on model clauses, or pursuant to an approved code of conduct or an approved certification. The Regulation specifies how consent can be properly obtained and, for the first time, identifies the age of consent in relation to the processing of personal data, which by default is 16 years, unless a member state legislates to an age not below 13 years.

The Regulation sets out detailed rights of individuals in relation to data processing, which includes the right to access your personal data, the right to rectification and the right to erasure of information where, for instance, the information is no longer necessary or consent has been withdrawn and there is no other legal ground. Other rights include the right to data portability, namely, to receive your personal data in a structured and commonly used format and the right to transmit this data to another controller, and the right to object to the processing of information. The scope of these rights can still be restricted on a wide range of grounds, including where there is a need to safeguard national security, defence and public security for the purpose of preventing, investigating, detecting or prosecuting crime or breach of ethics for regulated professions and for the enforcement of civil claims. Once adopted, breach of the Regulation could result in fines of up to 4 per cent of the organisation's annual worldwide turnover, or a maximum of 20 million euros (whichever is highest) for violations of any core principles of the new Regulation. This Regulation is to be formally approved in early 2016 and will enter into force in early 2018.

The Network and Information Security Directive, already being described colloquially as the 'Cybersecurity Directive', is primarily concerned with enhancing national cybersecurity capabilities, improving cooperation and applying security and notification requirements both for operators of essential services and for digital service providers. Under the Directive, member states must adopt a national network and information security strategy in line with EU law and designate a national supervisory authority and computer security incident response teams to handle risks and incidents. In terms of cooperation, an EU-wide 'Cooperation Group' will be established in order to facilitate cooperation and information sharing between member states. Both operators of essential services and digital service providers will be under an obligation to notify security incidents to the relevant national supervisory authority; the difference in their notification obligation remains to be seen. To a certain extent, the Directive leaves the precise definition of 'operators of essential services' and 'digital service platforms', such as e-commerce platforms, search engines and cloud services, to the discretion of member states.

The International Organization for Standardization's ISO 27001:2013 sets out standards, including requirements for the assessment and treatment of risks tailored to the needs of an organisation, as well as generic requirements applicable to all organisations. It includes standards of leadership and commitment to information security management by senior management, requirements for planning action, implementation and evaluation, and sets out requirements for resources, competence and awareness as well as proper communication and documentation of arising issues.

The ISO has not been formally adopted as a legal requirement to meet government standards, and is, in fact, insufficient to meet the 'UK Cyber Essential and Cyber Essentials PLUS' certificates (for more detail, see question 13). The Cyber Essentials scheme does, however, recommend the ISO to executive management, as supporting standards in addition to its own. Further, although there has been no formal adoption of these standards, if an organisation does adopt and apply them to its data operations, this would give comfort that in the event of a civil suit, civil penalty, or even in the event of a prosecution for a DPA offence, the organisation would be able to advance an arguable defence.

At present, aside from the general standards, in the ICT context, the Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR), implementing Directive 2002/58/EC, imposes obligations on a provider of public electronic communications services to take appropriate technical and organisational measures to safeguard the security of that service. The law does not seek to impose a standard as such: a measure shall only be taken to be appropriate if, having regard to the state of technological developments and the cost of implementation, it is proportionate to the risks against which it would safeguard. Administrative financial penalties can be imposed for breaches of the regulation (but they have so far been confined to marketing breaches with which the Regulations are also

concerned). It is expected that Directive 2002/58/EC and, thus, the PECR will be reviewed once the new Regulation has been implemented.

4 What are the obligations of responsible personnel and directors to keep informed about the adequacy of the organisation's protection of networks and data, and how may they be held responsible for inadequate cybersecurity?

Responsible personnel and directors have the normal obligations to act in the interests of those corporate bodies whom they represent in accordance with the law (as embodied in the DPA, as well as the Companies Act 2006 and elsewhere). For instance, pursuant to section 174 of the Companies Act 2006, a company director is held against the standard of 'a reasonably diligent person with [...] the general knowledge, skill and experience that may reasonably be expected of a person carrying out the functions carried out by the director in relation to the company [...]'. This is an objective test, which sits alongside a subjective test of knowledge, skill and experience. Personal liability could, therefore, follow in certain circumstances for breaches, where it is found that directors failed to fulfil those standards. The DPA also provides for liability of directors and officers for certain offences committed with the consent from, or that are attributable to, the negligence of the director, unless all due diligence has been exercised. However, there is no specific law with regard to cybersecurity. Ultimately, data protection liability rests with the organisation in question. The new EU Data Protection requirements will add further layers of corporate responsibility.

5 How does your jurisdiction define cybersecurity and cybercrime?

There are no legal definitions of cybersecurity and cybercrime as such: the thinking is certainly dominated by data protection concepts, but has now spread beyond that. The police define cybercrime as the use of any computer network for crime, and the National Crime Agency (NCA) define it as any crime committed through the use of information communication technology.

According to the NCA, the most common cyberthreats for businesses are hacking and DDoS. For consumers, they are larger in number: phishing (eg, bogus emails asking for personal details or delivering harmful viruses), webcam manager (taking over your webcam), file hijacking (hijacking files and holding them in ransom), keylogging (recording what you type on your keyboard), screenshot manager (taking screenshots of your computer screen) and ad clicker (directing a computer to click a specific link).

6 What are the minimum protective measures that organisations must implement to protect data and information technology systems from cyberthreats?

There are no minimum protective measures as such, except for compliance with the Seventh Data Protection principle or its equivalents. The standards at the level of law tend to be expressed by what is appropriate, measured against risks. More specific standards may be applied, in particular, implementations of the general standard (see ISO 27001).

See question 3 for the minimum measures likely to be required as a consequence of the General Data Protection Regulation.

See question 2 for reference to PCI DSS applied to cardholder data security.

7 Does your jurisdiction have any laws or regulations that specifically address cyberthreats to intellectual property?

While there are no specific laws or regulations addressing cyberthreats to intellectual property, it is protected both by criminalising the way in which it would be unlawfully obtained and by criminalising its improper use. One would also have to consider civil liability.

The main purpose behind offences listed in question 1 may perhaps not have been to protect intellectual property, per se, however, in reality, the obtaining of intellectual property by means of cyberattack would be covered by many of the offences under the CMA and the FA, notably fraud by false representation, given that the offence covers any act whereby an individual dishonestly makes false representations in order to make a gain or cause a loss. This can include purporting to be the person to whom the data relates or belongs.

The use of the data that has been misappropriated will often also be criminal. Section 107 Copyright Designs and Patents Act 1988 establishes a range of offences committed by those who for commercial purposes infringe copyright by making or dealing with infringing articles when they know or have reason to believe they are infringing. This is likely to catch individuals threatening intellectual property using cyber methodologies. The section is broad and encompasses a range of activity, including copying, distributing and, simply, communicating work to the public. Punishments for offences under this section vary in their maximum sentences, with the most severe offences carrying a maximum sentence of 10 years imprisonment and a fine.

8 Does your jurisdiction have any laws or regulations that specifically address cyberthreats to critical infrastructure or specific sectors?

Cyberattacks that are directed against the critical national infrastructure will be criminal if they meet the tests set out in the CMA (see question 1). Threats of this nature are also likely to represent threats to the UK's national security and, as such, those making them are liable to come to the attention of the UK's security and intelligence agencies and law enforcement authorities.

The SCA amended the CMA by creating an offence for persons to knowingly use a computer for an unauthorised purpose that causes or creates a significant risk of damage to human welfare, the environment, the economy and the national security of any country (section 3ZA CMA). The infrastructure and sectors this law seeks to protect from 'disruption' include energy, fuel and water, in addition to communication and transport networks and health services (section 3ZA(3)). Offences under this section where there is a significant risk of serious damage to human welfare or national security carry life-term prison sentences (section 3ZA(7)), and 14 years' imprisonment for any other offence under this section.

The CMA provisions for extraterritorial jurisdiction have been extended by the SCA to provide a legal basis to prosecute if there is a 'significant link' to the UK, namely, if the accused is in the UK at the time of the offence or if the affected computer is in the UK. Additionally, a UK national may also be prosecuted where there is no significant link to the UK, provided that the offence is an offence in the country where it took place (section 5 CMA, pursuant to article 12 of the EU Directive 2013/40/EU on attacks against information systems).

9 Does your jurisdiction have any cybersecurity laws or regulations that specifically restrict sharing of cyberthreat information?

There is nothing restricting private entities from sharing cyberthreat information, subject to standard questions of confidentiality. The government has been actively encouraging effective sharing in order to tackle cyberthreats and improve cybersecurity. The Cybersecurity Information Sharing Partnership (CiSP), a part of CERT-UK, was established as a joint industry government initiative to share information about cyberthreats and vulnerabilities. It includes members across all sectors and organisations, in order to exchange cyberthreat information in real time within a framework that protects confidentiality of shared information. The government has also set up industry-specific spaces, for example, the Retail Cyber Security Forum, to help address effective reporting and information sharing within an industry. It should also be noted that effective sharing of information is one of the aims of the EU draft Network and Information Security Directive.

To the extent that, in the context of sharing cyberthreat information, personal data forms part of that information, then obviously the requirements of the DPA must be met (see below).

Sections 19-21 of the Counter-Terrorism Act 2008 allow state authorities to share material intercepted under RIPA or other national security sensitive information with other intelligence services and also private entities if in pursuance of national security or the prevention of serious crime. Section 19 absolves any individual or entity for breach of confidentiality provided the threshold has been met where it is sharing information for national security purposes or for the prevention of serious crime.

There are limitations on the capacity to share information obtained by interception. Where a government agency has, under warrant, intercepted communications in the interests of national security or for the prevention of serious crime, notably from a telecommunications service provider, it is a criminal offence for a person in that service provider or for a public official to fail to keep secret the existence and content of the warrant or authorisation. Any information from that source therefore needs to be desourced. Other information from government bodies can be shared as long as it is compatible with their own statutory foundations (if any) and the requirements of the Human Rights Act 1998.

Article 8 of the ECHR (the right to privacy and freedom of correspondence) given effect in England through the Human Rights Act 1998, pervades this entire area insofar as privacy might be infringed by domestic public authorities, and limitations to that right must be in accordance with law, and proportionate and necessary only for the purposes prescribed in article 8(2), that is in the interests of national security or to prevent or detect crime (and others).

The DPA (see also question 1) regulates the use of 'personal data', that is data from which a living individual can be identified, which is retained on a computer (section 1(1)) and places duties on those persons responsible, known as 'data controllers', for processing that data (section 4(4)). Every data controller must comply with the data protection principles (set out in Part 1, Schedule 1), which ensure that personal data is obtained for a specific purpose and shall not be processed in any manner incompatible with that purpose (Part 1(2)) including by keeping the data secure.

It is an offence for any person to knowingly or recklessly obtain, disclose or procure the disclosure of personal data, in addition to selling or offering to sell such data that has been unlawfully obtained pursuant to section 55. Offences of this nature currently carry punishments by way of fines only. A civil penalty regime enforced by the Information Commission under section 55A DPA allows a civil monetary penalty of up to £500,000 (at the time of writing) to be imposed on a data controller guilty of serious breaches, as a means of encouraging good practice in the handling of personal data. The Parliamentary Justice Committee has considered proposals to amend the DPA further to include custodial sentences for the section 55 criminal offence, but none are presently available.

Further protection as to privacy is provided by RIPA as it is an offence for persons to intentionally and without lawful authority intercept any communication in the course of its transmission (section 1(1) and (2)) unless such conduct is permissible by way of a warrant issued by the Secretary of State in matters of national security, serious crime prevention, or in the safeguarding of the UK economy (section 5). Monitoring such communications is lawful if done by the provider of a telecommunications service, and it takes place for purposes connected with the provision or operation of that service, or with the enforcement, in relation to that service, of any enactment relating to the use of postal services or telecommunications services (section 3).

The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 set out exceptions where, in connection with the carrying on of a [private or public sector] business, the monitoring of communications will be authorised, for example, to establish the existence of facts or ascertain compliance with regulatory practices, and where such conduct is in the interests of national security or crime prevention. Interception upon these bases will not, therefore, contravene RIPA, even though they do not amount to exemptions from the DPA.

Where a private party is connected to civil proceedings (but is not directly involved), disclosure of information (eg, personal data) may be possible by an application to the court for a *Norwich Pharmacal* order. Unless there is a need for secrecy or urgency, an application should be made on notice to the respondent and the draft order should specify the information being sought, which may also impose a 'gagging order' to refrain the respondent from informing anyone about the application.

10 What are the principal cyberactivities that are criminalised by the law of your jurisdiction?

The CMA prohibits unauthorised access to computer material or data (ie, 'hacking' (section 1)). It is also an offence to carry out unauthorised acts designed to impair computer systems, which include the deployment of 'Trojan horses' or 'worms' (section 3). The latter offence can carry a prison sentence of up to 10 years and an unlimited fine on conviction in the Crown Court in England and Wales. It is also an offence to use or obtain for use articles in order to commit either of the first two offences mentioned. See also answers to questions 1 and 8.

The unauthorised interception of information (eg, through 'phone hacking') is covered by RIPA. A prison term of up to two years is provided for offenders under section 1(7)(a).

As above, section 55 DPA creates an offence for unlawfully obtaining and processing personal data. As an illustration of the sentences previously imposed, in February 2015, an online holiday insurance company was fined £175,000 by the ICO because of the IT security failings that resulted in the use of credit cards of 5,000 customers.

All these offences can be committed by a corporation, where liability can be attributed to such a legal person through the actions of its directors and officers and those who are senior enough to bind the corporation.

References to criminal offences are to be found in questions 1, 8 and 9.

11 How has your jurisdiction addressed information security challenges associated with cloud computing?

The DPA principles also apply to cloud computing services, most notably the Seventh, which specifies that an organisation must take steps to prevent unauthorised access as well as accidental loss of, or damage to, personal data (see question 1). The responsibility of ensuring adequate protection ultimately lies with the data controller, namely, the original holder or owner of the data. The same responsibility is also placed on the data processor, namely, the cloud service provider, where it has gained sufficient control over the manner in which the data is processed and is essentially treated as a data controller. The responsibility exists whether the data is being held or is in transit, and lies in mitigating security risks to ensure end-to-end security. This involves undertaking the necessary checks on the cloud service provider (by someone with appropriate technical expertise) to ensure it provides sufficient guarantees and takes reasonable steps to ensure compliance with the DPA. It should be noted that although responsibility in mitigating risks lies both in the holding and the transfer of data, most issues and most penalties have, so far, been with regard to data in transit. It should also be noted that the new Cybersecurity Directive will also apply to cloud-computing services, and will, thus, impose further obligations, for instance, the requirement to notify the national supervisory authority of any cybersecurity incidents.

The draft EU Regulation (see question 3) places responsibility not only on the data controller but also on the data processor for a range of obligations and liabilities. The proposals also impose certain additional rules on data processors, such as restrictions on international data transfers and further duties. These proposals are treated with caution and apprehension by commentators, who are concerned this will force cloud computing and other service providers out of the EU.

Further guidance has been published by the UK's Information Commissioner's Office on the Use of Cloud Computing (see https://ico.org.uk/media/for-organisations/documents/1540/cloud_computing_guidance_for_organisations.pdf). In 2012 the European Commission published 'Unleashing the Potential of Cloud Computing in Europe' through the European Cloud Computing Strategy and, in due course, cloud providers may well shoulder their own protection obligations, rather than solely the data controllers (see http://ec.europa.eu/digital-agenda/en/european-cloud-computing-strategy).

One of the difficulties is that the location of cloud computing service users is generally less well controlled and controllable. In a survey in June 2014, 75 per cent of consumers using social media on mobile devices stated they were automatically logged in from their personal devices, as were 23 per cent of mobile banking users. As a result, in addition to the application of the Cyber Essentials scheme (see question 13), additional precautions, such as a two-factor authentication, are greatly encouraged. There is a plethora of guidance, including the report from the ICO mentioned above, as well as the ISO27001: Information Security Management (see question 3).

As cloud computing often involves the movement of data to a 'cheaper jurisdiction' the user may not be aware of the physical location where it is stored. Personal data can only be transferred to a country outside the EEA if that country is on the Commission's authorised list of countries that provide adequate protection for personal data. The DPA permits organisations to transfer data to a non-EEA location where the organisation demonstrates that they meet the Binding Corporate Rules and satisfies the requirements of the 'Article 29 Working Party' (see https://ico.org.uk/for_organisations/data_protection/overseas/binding_corporate_rules). The Safe Harbour Agreement between EU states and the United States, stating the US did fulfil the necessary requirements for organisations to be permitted to transfer data, was held to be invalid by the European Court of Justice in October 2015 (*Max Schrems* case). That Safe Harbour agreement is presently being renegotiated, but alternative arrangements now available for organisations seeking to store data in the United States (pending a new Safe Harbour agreement) and other non-EEA states include doing this by contract or by express consent from the data subjects.

12 How do your jurisdiction's cybersecurity laws affect foreign organisations doing business in your jurisdiction? Are the regulatory obligations the same for foreign organisations?

As the EU is attempting to harmonise cybersecurity laws and regulations across member states, organisations in other EU states are likely to have very similar standards and obligations. However foreign organisations processing or storing personal data of any EU subjects outside the EU are likely to be prevented from doing business in the UK or with UK individuals if their security requirements and regulations are not sufficiently adequate, namely, equivalent to protection within the EU (following the recent case *Max Schrems* in the European Court of Justice) (see questions 3 and 11).

Best practice

13 Do the authorities recommend additional cybersecurity protections beyond what is mandated by law?

Yes. Much guidance has been issued by the UK government but ultimately the decision as to the level of security to be put in place remains an issue for organisations based on their assessment of risk to themselves and their customers underpinned by the legal requirements.

In implementing the UK government's Cyber Security Strategy (see question 18) the government has worked with industry to develop the Cyber Essentials scheme (www.gov.uk/government/publications/cyber-essentials-scheme-overview), which aims to give organisations a clear baseline to aim to protect themselves against the most common cyberthreats. Independent assurance schemes are available to demonstrate that the organisation in question has taken a considered approach and has met a government-approved standard, with a view to this giving a competitive edge over others who have not.

Other schemes include Cyber Streetwise (www.cyberstreetwise.com) and Get Safe Online (www.getsafeonline.org), which provide basic advice for individuals and businesses.

The government has tried to make it easy for organisations to improve cybersecurity. An example is to be seen in the launch of the Cyber Governance Health Check, which is a free service providing a confidential, tailored report for large organisations, enabling them to see what changes it should make. This has also enabled the government to aggregate data on how companies are performing.

14 How does the government incentivise organisations to improve their cybersecurity?

The government recently released a new scheme, Innovate UK, to encourage small businesses to improve their cybersecurity. Through this scheme it offers micro, small and medium sized businesses up to £5,000 for specialist advice on how to boost their cybersecurity.

Organisations bidding for central government contracts will need to be 'Cyber Essentials' certified.

In 2012 the UK government launched 'G-Cloud' so that public sector authorities could invite private sector organisations to carry out work without the need to resort to a formal tender process. Its success has resulted in the rebranding of this cloud service to the 'Digital Marketplace' (www.digitalmarketplace.service.gov.uk) together with the establishment of the Government Digital Services division of the Cabinet Office to assist the public sector in easily, securely and cost-effectively engaging the private sector, which must explain how their services meet the Cloud Security Principles in the procurement framework.

In November 2015, the government, through the organisation Ipsos MORI, launched a telephone survey seeking businesses' views on cybersecurity to provide up to date findings on their approaches, help organisations learn more about issues that businesses like theirs are likely to face, and inform government policy on cybersecurity and how they need to work with businesses to improve this area.

15 Identify and outline the main industry standards and codes of practice promoting cybersecurity. Where can these be accessed?

There is no equivalent of the IT Industry Council 'Cybersecurity Principles for Industry and Government' as has appeared in the US. In the UK, guidance appears piecemeal and is issued by individual companies. In addition, often, industry regulators will point to and suggest use of government report and advice, such as the 'Ten Steps to Cyber Security'.

See further questions 13, 14 and 27.

16 Are there generally recommended best practices and procedures for responding to breaches?

Best practice in this area is still under development and will be fact-specific. In the event of the loss of personal data obvious steps need to be taken to rectify the situation so as to seek to recover the 'lost' data and put in place measures to ensure there is no recurrence.

17 Describe practices and procedures for voluntary sharing of information about cyberthreats in your jurisdiction. Are there any legal or policy incentives?

There are no government requirements and no incentives as such, however, the government has tried to encourage the sharing of information about cyberthreats (see question 9). The government's encouragement towards collaboration is evidenced by the ICO's 'Protecting personal data in online services: learning from the mistakes of others' report (https://ico.org.uk/media/for-organisations/documents/1042221/protecting-personal-data-in-online-services-learning-from-the-mistakes-of-others.pdf).

18 How do the government and private sector cooperate to develop cybersecurity standards and procedures?

In 2011, the UK government issued an overarching UK Cyber Security Strategy (www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf), which seeks to put the UK in a position where:

> *law enforcement is tackling cyber criminals; citizens* [*including businesses*] *know what to do to protect themselves; effective cyber security is seen as a positive for UK businesses; a thriving cyber security sector has been established; public services online are secure and resilient; and the threats to* [*the UK*] *national infrastructure and national security have been confronted.*

This strategy recognises and requires the involvement of businesses to make it work.

A Cyber Growth Partnership (CGP), which is a joint initiative between industry, academia and government, aims at boosting the UK's global market position in cybersecurity products and services. Under that, a new Cyber Security Suppliers scheme has been developed, whereby businesses can show that they supply cybersecurity products and services to the UK government and use the government logo in their marketing material. The intention is to provide assurance to the private sector of the efficacy and operability of cyber-defence products. For instance, as part of the CGP, the UK Trade and Investment and the Department for Culture, Media and Sport set up a Cyber Demonstration Centre this year to support growth of this sector and be used to showcase services or products offered to various industries.

19 Is insurance for cybersecurity breaches available in the jurisdiction and is such insurance common?

Yes, in principle, insurance cover is available to mitigate cybersecurity risks as with any other risks. Unsurprisingly, the market is often considered generally underdeveloped given that the scale of risk to be insured against is uncertain on the basis that the risk of a cybersecurity breach and its detection (if it has occurred) and the assessment of the loss arising from a breach are difficult for brokers and underwriters to assess.

The UK government has recently been working with the insurance sector in order to highlight the important role of cybersecurity insurance and in an attempt to make the UK a world centre for cybersecurity insurance. On 5 November 2014, they issued a joint statement (www.gov.uk/government/uploads/system/uploads/attachment_data/file/371036/Cyber_Insurance_Joint_Statement_5_November_2014.pdf), emphasising the 'strong role' of cyber insurance in mitigating cyber risks, specifically in relation to 'malicious attacks'. A working group focusing on how cyber insurance can both mitigate damage caused by cyberattacks and encourage better cybersecurity by offering premiums for cyber-secure organisations released a report in March 2015 (www.gov.uk/government/uploads/system/uploads/attachment_data/file/415354/UK_Cyber_Security_Report_Final.pdf). This report notes the gap in awareness of the use of insurance, evidenced by the large number of firms unaware that insurance was even available; around 50 per cent of CEOs believed their companies have some form of coverage in place, but only 10 per cent of UK companies

Update and trends

During 2015, there has been yet greater attention to matters of cybersecurity. The autumn saw what was, arguably, at least in public relations terms, one of the biggest breaches so far in the case of TalkTalk, a provider of pay television, telecommunications, internet access and mobile network services to businesses and consumers in the United Kingdom. It has been reported that hackers breached security systems and stole significant amounts of customer data, following which they sought to blackmail the company into paying for its recovery. The incident led to the arrest of certain individuals, which was seemingly possible because of the prompt and close cooperation between TalkTalk and government agencies. It should be noted that TalkTalk did submit a breach notification to the ICO, as is required by the PECR. TalkTalk's chief executive officer was the subject of intense media attention and was called upon to defend the company and its cybersecurity practices.

The present trend appears to be for data that has been taken to appear on the 'dark web' where its presence, or the threat of its presence there, is used as a means of achieving extortion or reputational damage. Monitoring such spaces is now, arguably, a necessary part of cybersecurity activity. Whether or not the high-profile nature of the TalkTalk incident will change behaviour more widely across the technology industry and other industries remains to be seen, but 2015 was certainly a year where cybersecurity moved further up the business agenda. It is also fair to report that it is becoming ever more a mainstream business risk and recognised as such. One result of this is the increased role to be played by lawyers, both in terms of governance and the likelihood of litigation.

The implementation of amendments to the Computer Misuse Act 1990 through the Serious Crime Act 2015 has made the law of England and Wales consistent with the UK's EU obligations and introduced a suite of crimes, which, in the way they are framed, reflect the potential damage that could follow a cyberattack. They also reflect the UK government's policy of creating deterrent sentencing powers in the courts, for instance, by increasing the maximum sentence for cyberattacks that threaten life or the national security of the UK to life imprisonment. Of course, the implementation of the law does not make the investigation and prosecution of cyber crime any easier: the problems of attribution and the difficulties in gathering evidence, especially overseas, remain as they always did. Given that cyber crime is an international phenomenon, it remains to be seen how far the amended criminal law will prove to be a deterrent and how far the authorities in England and Wales will be able to investigate effectively and bring criminal cases before the courts. The concentration of investigative skill and resource in the National Crime Agency should assist in this process but is likely to lead to a lack of attention to 'lower level' attacks. Whatever the state of the criminal law, the message to businesses is clear: good business sense and the law in the form of the Data Protection Act require sound cybersecurity practices and the implementation of ISO 27001:2013, as well as adherence to the policies usefully made available by the UK government through its various public initiatives.

In legal terms, by far the biggest change is that foreshadowed by the agreement, after four years of negotiation, of the General Data Protection Regulation and the Directive with measures to ensure a high common level of network and information security: known as the 'Cybersecurity Directive'. The former seeks to redefine EU data protection law, acknowledging the current age of connectedness and the fact that the EU Charter of Fundamental Rights has given individuals a fundamental right to data protection. It provides real incentives to businesses to maintain cybersecurity, given the introduction of mandatory reporting obligations in the event of data breach and a severe penalty regime for failing to adequately protect personal data or otherwise breach the terms of the Regulation. The Regulation is user-friendly and efficient, for instance, in its provision that organisations with a presence in more than one state need only deal with the supervisory authority of the state of their main establishment (for further details see question 3). The proposed Directive sets out a programme requiring member states to increase their preparedness and improve their cooperation with each other, as well as requiring operators of critical infrastructures, including digital services, to adopt appropriate measures to manage security risks. The granularity of the requirements in the draft legislation is greater than ever before and will put in place, through the European Commission, a system of secure information sharing, early warnings, security requirements and incident notifications, among other things.

On the implementation of the new EU requirements in the UK, one might expect to see further and more detailed policy guidance emanating from the UK government, which remains an extremely active player. The announcement by the UK Chancellor of the Exchequer in his Autumn statement (which sets out the government's financial plans for the coming year) of significant resources to be applied in the cybersecurity field further demonstrated the importance that is attached to this subject.

actually had cyber insurance protection (as at March 2015). The report further provides a thorough assessment of the risks of and potential losses deriving from cyberattacks, as well as serious encouragement of the Cyber Essential scheme.

Enforcement

20 Which regulatory authorities are primarily responsible for enforcing cybersecurity rules?

In terms of cyberattacks, the law enforcement body with prime responsibility for investigations is the National Crime Agency, which has a dedicated cybercrime unit (www.nationalcrimeagency.gov.uk/about-us/what-we-do/national-cyber-crime-unit). As with other crimes, criminal cases would have to satisfy the criteria that would allow prosecution by the Crown Prosecution Service: a reasonable prospect of success and the public interest. In November 2015, the government announced a comprehensive programme including a National Cyber Centre, the country's first 'cyberforce'.

The Information Commissioner enforces the DPA in both criminal and civil jurisdictions (https://ico.org.uk/what_we_cover/taking_action/dp_pecr).

Where national security is at risk the UK's security and intelligence agencies will be involved.

In addition to enforcement by regulatory authorities, the DPA also makes provision for individuals to claim compensation in civil courts for damage and distress suffered as a result of data protection breaches.

21 Describe the authorities' powers to monitor compliance, conduct investigations and prosecute infringements.

The powers of the authorities to monitor and investigate for criminal offences under the CMA are the same as those in respect of criminal investigations generally. Material can be obtained by the NCA or the police through court orders (and searches without notice can be carried out with the appropriate permissions). Covert surveillance and interception are also possible, again with the necessary permissions having been obtained. It should be noted that intercept evidence is generally not admissible in criminal proceedings in England.

In data protection terms, the Information Commissioner may serve information notices requiring organisations to provide the Information Commissioner's Office with specified information within a certain time period; issue undertakings committing an organisation to a particular course of action in order to improve its compliance; serve enforcement notices and 'stop now' orders where there has been a breach, requiring organisations to take (or refrain from taking) specified steps in order to ensure they comply with the law; and serve assessment notices to conduct compulsory audits to assess whether an organisation's processing of personal data follows good practice.

22 What are the most common enforcement issues and how have regulators and the private sector addressed them?

There have been very few prosecutions of those responsible for cyberattacks. This is likely a consequence of the lack of a dedicated, well-resourced investigative unit, the prime purpose of which is the investigation and prosecution of cybercrime, however, that may change given the creation of the NCA Cyber Crime Unit. Further, the Metropolitan Police Commissioner, in December 2015, announced the creation of a task force of 500 police officers within the next year, who will specifically deal with cyber crime. The evidential difficulties of proving a criminal offence to the requisite standard are likely to be great especially given the likely problems in proving the origin of an attack and identifying a particular person or organisation responsible.

Most attention has been given to the Information Commissioner's powers under section 55A DPA although, even under those powers, there have

been few prosecutions: 13 prosecutions undertaken, of which 10 resulted in a criminal conviction and four cautions in the last year. The power to impose financial penalties was put in force in April 2010. Between that date and November 2015, the ICO has levied fines totalling £783,500, in relation to cybersecurity incidents (which may not be regarded as a significant figure in overall terms). A £250,000 fine was levied on Sony in January 2013 where it failed to put in place on its Network Platform adequate security measures, which meant personal data of a large number of individuals was lost in a (criminal) cyberattack on its network. In August 2014 the Ministry of Justice was fined £180,000 for failing to encrypt data concerning prisoners under its control. In November 2015, a penalty of £200,000 was imposed on the Crown Prosecution Service after laptops containing videos of police interviews were stolen from a private film studio (seemingly on the basis that the laptops were not encrypted).

23 What penalties may be imposed for failure to comply with regulations aimed at preventing cybersecurity breaches?

Civil actions under section 55A DPA can lead to penalties of up to £500,000.

24 What penalties may be imposed for failure to comply with the rules on reporting threats and breaches?

Generally there are no such reporting requirements, although a failure to report may well be considered an aggravating factor in the event action is taken by the Information Commissioner under section 55A DPA. This will obviously be subject to change when the General Data Protection Regulation comes into force (see question 3).

For public and electronic communications providers, there is a duty under the PECR to submit breach notifications to the ICO. Failure to do so can incur a fine of £1,000.

25 How can parties seek private redress for unauthorised cyberactivity or failure to adequately protect systems and data?

Actions can be taken under the DPA for breaches of the principles including the obligation for a data controller to apply appropriate measures to keep data secure. Alternatively, normal civil law torts will apply of which the most relevant are actions in breach of confidence and negligence (for failing to keep data secure).

Threat detection and reporting

26 What policies or procedures must organisations have in place to protect data or information technology systems from cyberthreats?

There are no set policies or procedures in law or pursuant to government policy that must be implemented. However, good practice would dictate that policies do exist and are implemented, and the lack of policies would almost inevitably give rise to a breach of the DPA and lead to enforcement action from the Information Commissioner (see questions 21 and 22).

27 Describe any rules requiring organisations to keep records of cyberthreats or attacks.

Although there is no legal obligation on an organisation to record cyberincidents, and while there is general mention of the importance of incident management, the recording of incidents or threats is not included in the Cyber Essentials accreditation or the Government guide on 'Ten Steps to Cyber Security' (www.gov.uk/government/uploads/system/uploads/attachment_data/file/73128/12-1120-10-steps-to-cyber-security-executive.pdf). It is, however, suggested in the ISO:27001 'control objectives' as a way of logging and monitoring an organisation's cyberspace.

It should be noted that this will change when the General Data Protection Regulation and the Network and Information Security Directive come into force (see question 3) as the Regulation imposes the obligation to keep record of any breaches of the Regulation.

28 Describe any rules requiring organisations to report cybersecurity breaches to regulatory authorities.

There are no rules in England, except for public electronic communications service providers. Under Regulation 5A PECR, these communication service providers must notify the ICO of any personal data breaches. In 2015 (up to 19 November), 143 breaches were reported under this Regulation (see questions 3 and 24). Although there is no legal obligation on data controllers to report breaches of security that result in loss, release or corruption of personal data, the Information Commissioner believes serious breaches should be brought to his attention. Further, the UK government has taken action to make the reporting procedure simple and straightforward by establishing integrated reporting tools.

There are numerous ways to report cybersecurity breaches, fine-tuned to meet the needs of specific organisations. For government agencies and other public bodies, the two organisations are CESG (originally Communications-Electronics Security Group) the information security arm of GCHQ (Government Communications Headquarters) and GOVCERT, the CERT for government and public sector bodies. For private companies and organisations, the two main reporting agencies are the National Cyber Crime Unit (a part of the NCA), and 'Action Fraud', an online national fraud reporting centre. The Cyber Incident Response scheme also exists, which provides access to industry expertise.

When the EU Data Protection Regulation comes into effect, all cybersecurity breaches will have to be notified to the national supervisory authority.

29 What is the timeline for reporting to the authorities?

See question 28.

30 Describe any rules requiring organisations to report threats or breaches to others in the industry, to customers or to the general public.

See question 28.

Michael Drury **mdrury@bcl.com**

51 Lincoln's Inn Fields
London WC2A 3LZ
United Kingdom

Tel: +44 207 430 2277
Fax: +44 207 430 1101
www.bcl.com

France

Merav Griguer and Dominique de Combles de Nayves
Dunaud Clarenc Combles & Associés

Legal framework

1 Summarise the main statutes and regulations that promote cybersecurity. Does your jurisdiction have dedicated cybersecurity laws?

France has no dedicated cybersecurity laws. The legal framework for cybersecurity is composed of several laws.

Law No. 2013-1168 of 18 December 2013 on Military Planning for the Years 2014 to 2019 and various provisions relating to defence and national security (the 2013 Military Planning Law) included in article L2321-1 et seq and article L1332-6-1 et seq of the French Defence Code provide that it is the responsibility of the state to ensure adequate security of vital operators' critical systems.

Under this law and these provisions, the state must:

- determine obligations, such as the prohibition of certain systems connected to the internet;
- implement detection systems by providers certified by the state;
- check the security level of critical information systems using an audit system; and
- in the event of a major crisis, it may impose the necessary measures on operators.

Decree No. 2015-351 of 27 March 2015 taken in application with the 2013 Military Planning Law sets forth the conditions under which the above-mentioned obligations of vital operators shall be implemented.

A second Decree adopted on the same date (Decree No. 2015-350 of 27 March 2015) sets forth the procedure of certification of certain detection systems and of service providers of such detection systems, as well as of service providers authorised to control the security systems of vital operators.

According to article L1332-6-2 of the Defence Code, vital operators are required to report incidents to the relevant authorities to give advance warning to companies potentially affected by the same type of attack.

The 2013 Military Planning Law included in article L246-1 et seq of the Homeland Security Code provides that the intelligence services of the Ministries of Defence, the Interior, the Economy and the Ministry for the Budget may access personal information and data connections (including location-based mobile terminals, such as smartphones in real time) stored by electronic communications operators, ISPs and hosts, for the following reasons:

- searching information relating to national security;
- safeguarding essential elements of France's scientific and economic potential; and
- prevention of terrorism, organised crime and the prevention of dissolved groups reforming.

According to article 34 of the French Law No. 78-17 of 6 January 1978 on Data Processing, Data Files and Individual Liberties, a data controller shall take all useful precautions, with regard to the nature of the data and the risks of the processing, to preserve the security of the data and, in particular, prevent their alteration and damage, or access by unauthorised third parties.

Article 38 of Government Order No. 2011-1012 of 24 August 2011 implementing the European Telecom Package directives (Directive 2009/136/EC and Directive 2009/140/EC of the European Parliament and of the Council of 25 November 2009), and included in article 34b of the French Law No. 78-17 of 6 January 1978 on Data Processing, Data Files and Individual Liberties, provides that security breaches (any breach of security leading accidentally or unlawfully to destruction, loss, alteration, disclosure or unauthorised access to personal data processed in the context of providing electronic communication services to the public) should be notified immediately to the French data protection authority, the National Commission on Computers and Civil Liberties (CNIL).

Article 34b also provides that if a violation is likely to breach personal data security or the privacy of a subscriber or any other individual, the provider shall also immediately notify the affected party.

Only providers to the public of electronic communication services using electronic communication networks with open public access, referred to in article L33-1, paragraph 1 of the Post and Electronic Communications Code, are concerned by this new requirement. They must establish an inventory of violations and keep it available to the CNIL.

Articles 31 and 32 of the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data of 25 January 2012 (the General Data Protection Regulation) extends for all data controllers the obligation to notify the personal data breach to the supervisory authority and to inform data subjects of a personal data breach. These provisions set the specific terms of the new obligation to notify personal data breach.

Article 34-1 of the Post and Electronic Communications Code provides that technical data (such as logs, connection time and duration of the connection, the IP address, etc) must be retained for one year for the purposes of research, recognition and prosecution of criminal offences or breach of obligation under article L336-3 of the Intellectual Property Code (see question 7) or for the purposes of preventing harm to automated data processing systems in order to keep them available to the competent authorities.

Law No. 2014-1353 of 13 November 2014 strengthens provisions on the fight against terrorism, strengthens the repression of advocating terrorism and incitement to terrorism (article 421-2-5 of the Penal Code) and allows the competent government authorities to block websites advocating terrorism or inciting it. Pursuant to the provisions of this law, following a notification by the competent authority, the editor or host of the website in question shall remove the infringing contents within 24 hours. In the case of non-compliance within the said deadline, the network provider shall block forthwith the internet access to the website.

The specific conditions and guarantees under which the blocking of websites by the competent authorities shall be allowed are provided by Decree No. 2015-125 of 5 February 2015. The competent authority deciding on the necessary blocking measures is the Central Office for the Fight against Crime connected to Technologies of Information and Communication, under the control of the National Police Board.

Pursuant to the provisions of this law, following a notification by the competent authority, the editor or host of the website in question shall remove the infringing contents within 24 hours. In the case of non-compliance within the said deadline, the network provider shall block forthwith the web access to the website.

The specific conditions and guarantees under which the blocking of websites by the competent authorities shall be allowed are provided by Decree No. 2015-125 of 5 February 2015. The competent authority deciding on the necessary blocking measures is the Central Office for the Fight against Crime connected to Technologies of Information and Communication, under the control of the National Police Board.

Following the Paris terrorist attacks of January 2015 and November 2015, a series of laws have been adopted for the purpose of prevention and fight against terrorism. More specifically, Law No. 2015-912 of 24 July 2015 on intelligence aims to strengthen the capacities of the specialised intelligence services by permitting the use of intelligence gathering techniques already permitted within the judicial framework, especially including computer data capture. The Law on Intelligence introduced an obligation of certain network providers to install automatic detection systems allowing the monitoring of individuals identified as posing a terrorist threat. The implementation of all intelligence measures is subject to the prior consulting of the National Committee for Controlling Intelligence Techniques.

Law No. 2015-1556 of 30 November 2015 sets forth the legal framework allowing the surveillance of international electronic communications, namely, of electronic communications received or emitted between France and third countries. The surveillance may concern both connection data and the communications' content, and is subject to the authorisation of the Prime Minister or his delegates. Collected data can be only maintained during a limited time period, which shall not exceed 12 months for content data and six years for connection data.

2 Which sectors of the economy are most affected by cybersecurity laws and regulations in your jurisdiction?

The main sectors of the economy affected by cybersecurity laws and regulations are the telecoms, energy, water, hazardous installations, health, defence and arms sectors.

3 Has your jurisdiction adopted any international standards related to cybersecurity?

Although the International Organization for Standardization's ISO 27001:2013 is recognised by experts as one of the best practices for the protection of information systems, French laws have not expressly adopted such standard.

4 What are the obligations of responsible personnel and directors to keep informed about the adequacy of the organisation's protection of networks and data, and how may they be held responsible for inadequate cybersecurity?

Under article 34 of Law No. 78-17 of 6 January 1978 on Data Processing, Data Files and Individual Liberties (French Data Protection Act), the data controller shall take all useful precautions, with regard to the nature of the data and the risks of the processing, to preserve the security of the data and, in particular, prevent their alteration and damage, or access by non-authorised third parties.

Data controllers processing personal data without implementing the measures prescribed above are punishable by article 226-17 of the French Criminal Code by five years' imprisonment and a €300,000 fine.

5 How does your jurisdiction define cybersecurity and cybercrime?

The French Network and Information Security Agency of the Prime Minister (ANSSI), placed under the authority of the Prime Minister and attached to the Secretary General for National Defence, has defined 'cybersecurity' in an official document entitled 'Information systems defence and security – France's strategy' as:

> [*t*]*he desired state of an information system in which it can resist events from cyberspace likely to compromise the availability, integrity or confidentiality of the data stored, processed or transmitted and of the related services that these systems offer or make accessible.*
>
> *Cybersecurity makes use of information systems security techniques and is based on fighting cybercrime and establishing cyberdefence.*

6 What are the minimum protective measures that organisations must implement to protect data and information technology systems from cyberthreats?

The ANSSI has published a guide titled '40 Essential measures for a healthy network'. In particular it recommends that an organisation:

- keeps an up-to-date map of its IT system and users;
- upgrades its software;
- limits the number of internet access points to those that are strictly necessary;
- requires user authentication;
- uses secure terminal equipment; and
- inside the network, monitors systems, secures network administration, controls access to the premises and physical security, and organises the reaction in the case of fire.

The ANSSI also recommends providing passwords of sufficient strength. A password must contain at least eight characters and include numbers, letters and special characters. It must be renewed every 90 days. An employee must be technically forced to choose a different password from the three that he or she has used previously. At the first login, the password that was communicated to him or her by the administrator must be changed by the employee.

The General Security Repository (RGS) was created by section 9 of Ordinance No. 2005-1516 of 8 December 2005 on electronic exchanges between users and administrative authorities and between administrative authorities. The RGS is a repository for secure electronic exchange of public organisations.

The CNIL has also published two IT risk management guides (a general security guide published in 2010 and an IT risk management guide handling privacy issues published in 2015) with the aim of ensuring the protection and security of personal data. In 2015, the CNIL published two more guides on Privacy Impact Assessment, completing and updating the existing risk management guides.

7 Does your jurisdiction have any laws or regulations that specifically address cyberthreats to intellectual property?

Article L336-3 of the Intellectual Property Code provides that the person providing access to communication services to the online public has an obligation to ensure that such access will not be subject to use for reproduction, representation, making available or communication to the public of works or objects protected by copyright or related right without the required authorisation of copyright holders.

8 Does your jurisdiction have any laws or regulations that specifically address cyberthreats to critical infrastructure or specific sectors?

Critical infrastructure operators are more specifically regulated by cybersecurity laws, such as the 2013 Military Planning Law included in article L2321-1 et seq and article L1332-6-1 et seq of the French Defence Code. The telecoms sector in particular is concerned by data breach notification requirements.

9 Does your jurisdiction have any cybersecurity laws or regulations that specifically restrict sharing of cyberthreat information?

Article 226-15 of the Criminal Code prohibits the malicious opening, destroying, delaying or diversion of correspondence sent to a third party or fraudulently gaining knowledge of it. Such acts are punishable by one year's imprisonment and a fine of up to €45,000.

Article 226-1 of the Criminal Code prohibits the recording of private communications without the consent of the concerned person.

10 What are the principal cyberactivities that are criminalised by the law of your jurisdiction?

The principal cyberactivities that are criminalised by French law are intrusions into an information system, removal or alteration of data, breach of data, such as passwords, e-mail addresses and home addresses, the infection of a company's network by a Trojan horse, telephone tapping or call recordings, theft of computer files and documents, theft of digital identity and phishing attacks.

11 How has your jurisdiction addressed information security challenges associated with cloud computing?

The French data protection authority, the CNIL, considers that data subjects suffer from a lack of security and transparency on the part of cloud service providers. In June 2012, the CNIL published recommendations for companies planning to use cloud computing services:

- clearly identify the data and processing operations that will be hosted in the cloud;
- define the company's requirements for technical and legal security;

- carry out a risk analysis to identify security measures essential for the company;
- identify the relevant type of cloud for the planned processing;
- choose a service provider offering sufficient guarantees (in particular by assessing the level of protection provided by service provider for data processed);
- review the internal security policy; and
- monitor changes over time.

The CNIL also describes the essential provisions that should appear in a cloud computing service contract.

Moreover, the European Commission works with industry to agree on a code of conduct for cloud computing providers. Following the opinion of the Article 29 Working Party adopted on 22 September 2015, the Code of Conduct is currently being finalised by the Cloud Select Industry Group (C-SIG),

12 How do your jurisdiction's cybersecurity laws affect foreign organisations doing business in your jurisdiction? Are the regulatory obligations the same for foreign organisations?

In general, the laws relating to cybersecurity are applicable to foreign organisations.

Concerning the French Data Protection Law, it applies to processing of personal data bya data controller established on French territory, whatever its legal form, and to processing of personal data by a data controller, even though it is not French, or in any other member state of the European Union, using a means of processing located on French territory, unless the processing is merely for the purposes of transit through this territory or that of any other member state of the European Union.

Concerning the provisions of cybersecurity laws included in the Criminal Code, French criminal law is applicable to offences committed on the French territory. Pursuant to article 113-2 of the Criminal Code, the offence is deemed to have been committed on the French territory when one of its constituent facts took place in that territory.

Best practice

13 Do the authorities recommend additional cybersecurity protections beyond what is mandated by law?

The ANSSI published a guide titled '40 Essential measures for a healthy network' in 2013.

The ANSSI also published in October 2014 a security recommendation regarding analysis of https flows.

The CNIL has also published two IT risk management guides (a general security guide published in 2010 and an IT risk management guide handling privacy issues published in 2015) with the aim of ensuring the protection and security of personal data. In 2015, the CNIL published two more guides on privacy impact assessment, completing and updating the existing risk management guides.

14 How does the government incentivise organisations to improve their cybersecurity?

Not applicable.

15 Identify and outline the main industry standards and codes of practice promoting cybersecurity. Where can these be accessed?

The ANSSI has published on its website (www.ssi.gouv.fr) a classification method for industrial monitoring systems and the key measures to improve their cybersecurity, as well as a detailed description of applicable cybersecurity measures.

These documents do not have the force of law.

16 Are there generally recommended best practices and procedures for responding to breaches?

In July 2012 the CNIL published guidelines for managing the risks that personal data processing can generate in relation to individuals, proposing a list of good security practices. The French authority provides in particular measures to be implemented to handle breaches of personal data, overseeing the protection of privacy and reducing software vulnerabilities. The best practices aim to have an operational organisation to detect and deal with events likely to affect the freedoms and privacy of the individuals concerned. Measures include:

- providing employees and customers with required information;
- definition of roles and responsibilities of the persons in charge of responding to breaches;
- reporting procedure and reaction in the case of violation of personal data,
- action plan in the case of violation;
- inventory of data breaches; and
- improving security measures.

The above guidelines are completed and updated by a privacy impact assessment (PIA) published in 2015, in order to take into account the provisions of the upcoming European regulation on personal data. The PIA is composed by a method guide and a tool guide aiming to enhance the efficiency of the existing risk management methods.

17 Describe practices and procedures for voluntary sharing of information about cyberthreats in your jurisdiction. Are there any legal or policy incentives?

CERT-FR (the government centre for monitoring, warning of and responding to cyberattacks) publishes alerts, which are documents intended to prevent immediate danger, and opinions, which are documents outlining vulnerabilities and ways to guard against attacks.

18 How do the government and private sector cooperate to develop cybersecurity standards and procedures?

French governmental entities work with industrial stakeholders, such as final users, vendors, integrators and professional organisations. They are part of a working group, driven by the ANSSI. The aim is to set out concrete and practical proposals to improve the cybersecurity of critical infrastructures.

19 Is insurance for cybersecurity breaches available in the jurisdiction and is such insurance common?

Insurance for cybersecurity breaches has been increasing; however, this is still a fairly new concept and is, therefore, not yet common.

Enforcement

20 Which regulatory authorities are primarily responsible for enforcing cybersecurity rules?

The CNIL enforces compliance with information security rules relative to the French Data Protection Act.

The ANSSI or the public body appointed by the Prime Minister or service providers qualified by the Prime Minister may be responsible for enforcing cybersecurity rules applicable to vital operators.

21 Describe the authorities' powers to monitor compliance, conduct investigations and prosecute infringements.

The CNIL has the power to monitor compliance with the French Data Protection Act by data controllers on-site and their premises and those of their subcontractors. The French authority has also the power to sanction and to make its sanctions public (warnings, fines, injunctions to stop the data processing, etc).

The monitoring of vital operators is carried out by the ANSSI or by a public body appointed by the Prime Minister or service providers qualified by the Prime Minister. The cost of monitoring is borne by the operator.

22 What are the most common enforcement issues and how have regulators and the private sector addressed them?

The notification by telecoms operators of security breaches to the CNIL presents some difficulties. Indeed, by notifying security breaches the telecoms operator discloses security vulnerabilities. However, the CNIL may publish this information and even punish the company that notifies. Thus, the current system does not encourage the disclosure of such breaches.

23 What penalties may be imposed for failure to comply with regulations aimed at preventing cybersecurity breaches?

Failing to comply with the security requirements of the French Data Protection Act is punishable by a fine of up to €300,000. Article 226-17 of the French Criminal Code punishes data controllers who process personal

data without implementing the security measures by five years' imprisonment and a €300,000 fine.

24 What penalties may be imposed for failure to comply with the rules on reporting threats and breaches?

According to article L1332-7 of the Defence Code, vital operators failing to comply with the rules of reporting threats and breaches are punishable by a fine of €150,000. For legal entities the fine can be up to €750,000.

25 How can parties seek private redress for unauthorised cyberactivity or failure to adequately protect systems and data?

Parties may seek private redress for unauthorised cyberactivity or failure to adequately protect systems and data. Indeed, failure to fulfil these legal obligations constitutes a fault. The parties are, therefore, justified in claiming compensation for damage caused by the fault under article 1382 of the French Civil Code.

Threat detection and reporting

26 What policies or procedures must organisations have in place to protect data or information technology systems from cyberthreats?

Organisations must have the following policies and procedures to protect data or information technology systems from cyberthreats:

- a privacy and security policy;
- a code of conduct on good practice to prevent security breaches;
- internal procedure to report data breach;
- a computer clearances and permissions-management policy to restrict access to different databases to those with a legitimate interest;
- logging and archiving of computer access;
- passwords containing at least eight characters and including numbers, letters and special characters, which must be renewed every 90 days;
- use of encryption solutions based on strong well-known algorithms; and
- measures to ensure the availability, integrity and confidentiality of personal data.

27 Describe any rules requiring organisations to keep records of cyberthreats or attacks.

According to article 34b of the French Data Protection Act, each provider of electronic communication services must keep an updated record of all breaches of personal data, listing in particular the conditions, effects and measures taken as remedies, and must make this record available to the CNIL upon request.

28 Describe any rules requiring organisations to report cybersecurity breaches to regulatory authorities.

The obligation to notify personal data breaches to the CNIL concerns only electronic communications service providers to the public, as defined by article L33-1 of the Post and Electronic Communications Code, such as internet service providers and fixed and mobile telephony operators.

The cyberthreats or incidents concerned are destruction, loss, alteration, disclosure or unauthorised access to personal data by accidental or unlawful means.

The adoption of the European Regulation on personal data may impose a modification of the above-mentioned provision, given that the Regulation proposal of 2012 extends the obligation of notification to all data controllers.

29 What is the timeline for reporting to the authorities?

The notification must be submitted to the CNIL within 24 hours of the finding of the violation. An additional notification could be made within 72 hours of the initial notification. The notification can be made online.

30 Describe any rules requiring organisations to report threats or breaches to others in the industry, to customers or to the general public.

In the case of breach of personal data security or the privacy of a subscriber or any other individual, the provider must notify the party affected forthwith, unless the CNIL has found that appropriate protection measures have been implemented by the service provider to ensure that the personal data are made undecipherable to any unauthorised individuals and have been applied to the data affected by this breach.

DUNAUD CLARENC COMBLES & ASSOCIÉS
ASSOCIATION D'AVOCATS

Merav Griguer **merav.griguer@dcc-associes.com**
Dominique de Combles de Nayves **dominique.combles-nayves@dcc-associes.com**

4 Avenue Hoche
75008 Paris
France

Tel: +33 1 43 18 83 90
Fax: +33 1 40 54 05 15
www.dcc-associes.com

Germany

Svenja Arndt
ARNDT Rechtsanwaltsgesellschaft mbH

Legal framework

1 Summarise the main statutes and regulations that promote cybersecurity. Does your jurisdiction have dedicated cybersecurity laws?

In Germany, currently, there is no single dedicated cybersecurity law, however, cybersecurity provisions are spread throughout various single acts, which have partly been changed by an IT Security Act, which came into force in July 2015. The main statutes currently dealing with cybersecurity are the following.

Act on the Federal Office for Information Security (BSIG)
According to the changes in 2015, the BSIG has now two focuses. As previously in the past, it specifies the tasks of the Federal Office (BSI), which are to prevent threats to the security of federal IT (ie, technology operated by or on behalf of federal authorities and used for communication or data exchange among federal authorities or with third parties), to advise and to provide support to federal bodies including police, prosecution authorities, the Federal Intelligence Service and also to the federal states in Germany and to study security risks associated with the use of IT and develop security precautions (eg, cryptographicsystems for federal IT). In addition, it also provides information on risks and threats relating to the use of information technology for manufacturers, distributors and users of IT and seeks out appropriate solutions. It warns of malware and security leaks in IT products and services. This work includes IT security testing and assessment of IT systems, including their development, in cooperation with industry. It also issues security certificates and accredits IT products and services. With regard to critical information infrastructure (KRITIS) the BSI now also serves as the central reporting office. It analyses cybersecurity threats and their potential impact and informs and advises operators of KRITIS.

The new additional focus of this Act is now on operators of KRITIS. Within two years after the enactment of an ordinance still to be adopted they have to implement and regularly prove to the BSI technical and organisational measures against disruption of availability, integrity, authenticity and confidentiality of its IT systems. In the case of serious IT incidents they have to notify the BSI.

Telecommunications Act (TKG)
'Telecommunications' in the TKG means the technical process of sending, transmitting and receiving signals by means of telecommunications systems (ie, technical facilities or equipment capable of sending, transmitting, switching, receiving, steering or controlling electromagnetic or optical signals identifiable as messages). The TKG aims at promoting competition and efficient infrastructures in telecommunications and guaranteeing appropriate and adequate services throughout Germany. This includes, inter alia, safeguarding telecommunications privacy and provisions for telecommunications service providers on cybersecurity.

Telemedia Act (TMG)
The TMG is applicable for all electronic information and communication services insofar as they are not telecommunication services pursuant to the TKG, which consist entirely in transmitting signals via telecommunication networks, telecommunications-based services according to the TKG or broadcasting pursuant to the Interstate Agreement on Broadcasting. Telemedia service providers are not obliged to supervise the information transmitted or stored by them or to search for circumstances that indicate an unlawful action. But the obligations to erase or block information according to general laws remain. Also, telecommunications privacy pursuant to the TKG must be protected by technical and organisation measures to protect its technical facilities against unlawful access and attacks, specifically by using encryption.

Federal Data Protection Act (BDSG)
Next to these provisions applicable for specific areas, the BDSG lays down provisions on data protection of identified and identifiable natural persons. To secure their data the BDSG asks for technical and organisational measures to ensure the implementation of and adherence to the privacy provisions laid down in the BDSG, including cybersecurity measures. These provisions are also applicable for other provisions that refer specifically to the BDSG.

In addition, in July 2014 the Energy Industry Law (EnWG) was amended by specific provisions on ensuring cybersecurity protection measures for operators of energy plants and energy nets.

Next to these laws and acts in which cybersecurity is more or less addressed specifically there are rather general provisions for companies in relation to risk management systems. For example, pursuant to the German Act on Control and Transparency in the Corporate Sector (KonTraG) every company active on the capital market has to have a system for the early recognition of risks and has to publish the risks in the annual company financial statements. Similarly, companies within the scope of the Sarbanes-Oxley-Act (SOX) have to follow similar rules. Although the Act does not provide specifically for IT security measures, such as ISMS, conformity with the SOX is only possible with a robust IT security system. Also the Accounting Law Modernisation Act (BilMOG), the Act with which the European EuroSOX has been transferred to German Law, asks companies to lay down the main features of their internal control system in the annual company financial statements.

Among other laws, the German Banking Act (KWG), in section 25a, obliges banking institutions to have appropriate technical and organisational systems and an appropriate emergency concept, specifically for IT systems. The supervisory authority, BaFin has set up 'minimum requirements to the risk management' (MaRisk), which are the internal transformation of the requirements of Basel II and Basel III. According to these, banking institutions have to take care that their IT system and IT processes secure the integrity, availability, authenticity and confidentiality of the data. Therefore, the BaFin asks for adherence with the general standards, namely those of the BSI and ISO 27001 but also additionally for specific regulations on strategies, change processes and outsourcing.

There are similar provisions for the German Securities Trading Act (WpHG) and in the insurance sector.

2 Which sectors of the economy are most affected by cybersecurity laws and regulations in your jurisdiction?

Sectors falling into the scope of critical infrastructure are mainly affected, in particular the telecommunications and telemedia industry sectors and the banking sector. Outside these specific areas there are sectors that are vulnerable to cybercrime due to their know-how or products and are thus generally aware of the needs to cybersecurity. According to the 2015 report on cybersecurity of the BSI, industrial production sites have to face an increase in attacks. Also, public institutions, including the German parliament, are increasingly targets of cybersecurity attacks.

3 Has your jurisdiction adopted any international standards related to cybersecurity?

In Germany ISO 27001:2013 is widely spread, although not mandatory by law. As mentioned above, supervisory authorities may refer to that standard (eg, the BaFin in the banking sector). In addition, a certificate of adherence to ISO 27001 is very often requested by customers from service providers in the IT sector, for example, cloud service providers, and other kinds of data processing services on behalf of the controller.

In Germany, we have, in addition, the 'IT Basic Security Catalogues' applicable to various aspects of an IT landscape. They define precise measures that have to be complied with in the case of low or middle protection needs. For systems with high protection needs the Catalogues provide for a structured procedure to identify the necessary measures.

4 What are the obligations of responsible personnel and directors to keep informed about the adequacy of the organisation's protection of networks and data, and how may they be held responsible for inadequate cybersecurity?

Obligations of personnel mainly derive from general liability rules for damages resulting from intentional or negligent non-compliance to legal provisions or from general provisions on risk management, for example, in corporate law (Stock Corporation Act, KonTraG), the banking sector (KWG, etc). The MaRisk in the banking sector, or the KonTraG, for example, state that the management is responsible for all main risks.

5 How does your jurisdiction define cybersecurity and cybercrime?

Cybersecurity

Article 2 of the BSI Act defines 'security of information technology' as 'compliance with certain security standards for the availability, integrity, or confidentiality of information, by means of security precautions in information technology systems, components or processes, or for the use of information technology systems, components or processes'.

According to the 'old' DIN 44300 data, security was defined as a situation in which data are directly or indirectly as far as possible saved from impairments or misuse, namely taking into consideration non-processing-related risks as well as risks in the course of data processing services.

The BDSG includes data security as a part of data privacy by stating that public and private bodies that collect, process or use personal data on their own behalf or on behalf of others shall take the necessary technical and organisational measures to ensure the implementation of the provisions of the BDSG, especially the requirements listed in the Annex to the BDSG. These include measures on access control, virtual access control, disclosure control, input control, job control, availability control and client separation. Therefore data privacy and data/cybersecurity are partly overlapped, although data privacy must also be secured outside IT usage and IT security goes beyond protecting personal data.

Cybercrime

For cybercrime there is no official statutory definition. The Federal Criminal Police Office (BKA) has distinguished in its 'Federal Situation Survey 2011' between cybercrime in a narrow and in a broader sense. According to these definitions, cybercrime in the narrow sense is related to special phenomenon and form of this criminality, in which elements of electronic data processing are relevant for the performance of the offence. This includes crimes such as computer fraud, fraud with access authorisation to communication services, forgery of evidentiary data, deception in legal transactions while processing data, data tampering, computer sabotage, and data espionage, including preparatory actions. Cybercrime in a broader sense includes offences for which the internet is used as a means or for preparatory purposes, such as phishing in the area of online banking, crimes with DDoS attacks, all kinds of digital blackmailing, producing, granting, distributing or obtaining hacking tools, which are determined to be used for illegal purposes. These offences are not treated as cybercrime in the police statistics.

6 What are the minimum protective measures that organisations must implement to protect data and information technology systems from cyberthreats?

In the past, generally, no specific measures have been mentioned in German legislation. Although the laws, generally, still describe the measures in a rather generic way and allow either the users themselves or supervisory authorities to define specific measures, more specific measures were implemented in July 2014 for providers of telemedia and telecommunication services. In addition a new ordinance is planned, which will lay down details of protective measures for other operators of KRITIS.

In the telecommunications sector, the TKG states that every service provider has to take appropriate measures to protect the privacy of telecommunications and personal data and telecommunications and data processing systems against unauthorised access. For this purpose it is now specifically allowed to use customer and traffic data to detect, limit and eliminate failures of its service, including unauthorised access. Providers of publicly available telecommunication services have, additionally, to take appropriate technical measures on telecommunications and data processing systems operated for such purpose in order to protect against any faults that would result in considerable harm to telecommunications networks, also insofar as they can be caused by external attacks and the effects of natural disasters as well as to control the risk for the security of telecommunication networks and services. Measures have to be taken to secure telecommunications and data processing systems against unauthorised access and to limit the consequences of security breaches for users or for connected networks as far as possible. In addition, such providers have to nominate a security commissioner and draw up a security policy, which has to be submitted to the regulatory authority, the Federal Network Agency.

The BSI can set minimum standards for the protection of IT technology of the federal authorities. The Federal Minister of the Interior can lay down such standards as general administrative regulations for all federal authorities and offices. It can also warn the general public on security risks and recommend protective products.

In addition, the Federal Network Agency together with the BSI and the Federal Data Protection Commissioner have created a catalogue of security provisions for the operation of telecommunications, the data processing systems and the processing personal data as a basis for the security concept as well as for the necessary technical and other measures. This catalogue is published by the Federal Network Agency.

The BDSG generally asks for technical and organisation measures to ensure adherence to the provisions on data privacy as laid down in question 1.

7 Does your jurisdiction have any laws or regulations that specifically address cyberthreats to intellectual property?

Yes, for example, pursuant to the German Copyright Law it is forbidden to circumvent effective technological measures that protect a 'protected work' (according to this Act; including computer programs and databases) without the consent of the rightholder where the person acts in the knowledge or with reasonable grounds to know that circumvention is taking place in order to facilitate access to such a protected work or its exploitation. Technological measures are defined as technologies, devices and components that are designed to prevent or restrict acts that are not authorised by the rightholder. They are deemed effective where the use is controlled by the rightholder through application of an access control, a protection process, such as encryption, scrambling or other transformation, or a copy-control mechanism, which achieves the protection objective. The production, import, distribution, sale, rental, advertising and possession for commercial purposes of devices, products or components, as well as providing services, which are the subject of sales promotions, advertising or marketing with the aim of circumventing effective technological measures, apart from circumventing effective technological measures that only have a restricted economic purpose or benefit or that are mostly drafted, produced, adjusted or provided in order to facilitate or make easier the circumvention of effective technological measures.

There are specific criminal and administrative offences defined for breach of copyright, which can be penalised by imprisonment of up to three or five years or fines (for administrative offences of up to €10,000).

Disclosure of trade and company secrets (sections 17, 18 UWG) can be sentenced with imprisonment not exceeding three years or a fine.

8 Does your jurisdiction have any laws or regulations that specifically address cyberthreats to critical infrastructure or specific sectors?

With the new IT Security Act, specific provisions have been implemented into the BSI Act for critical infrastructure. These are defined institutions, plants and parts thereof in the energy, information technology and telecommunication, transport and traffic, health, water, nutrition and finance and insurance sectors, which are of high importance for the community.

However, further details on who will specifically fall under this definition will only be laid down in future in a separate ordinance. Operators of such critical infrastructure need to implement technical and organisational measures ensuring cybersecurity. But again, details will be laid down in a separate ordinance. In addition, operators need to notify the BSI of actual or feared infringements (in certain cases an anonymous notification is possible).

So far, the IT security level for critical infrastructure varies greatly. Some sectors have a distinct risk management, comprehensive security concepts, carry out audits, and participate in information exchange and training sessions. In others, such measures do not exist or are only rudimentary.

In addition, sectors or companies dealing with classified documents are specifically supervised by the Federal Ministry for Economic Affairs. According to the Security Clearance Check Act this Ministry is responsible for the protection of secrecy in commerce. It serves the purpose of establishing, maintaining and performing all measures necessary to protect and to keep classified information confidential. Based on the General Administrative Regulations the Ministry of Economic Affairs has laid down specific measures and rules for access to classified information in a Handbook on the Protection of Secrecy. This also includes a provision for IT systems to secure confidentiality as well as the integrity of classified documents.

9 Does your jurisdiction have any cybersecurity laws or regulations that specifically restrict sharing of cyberthreat information?

Besides the general Data Protection Act, whose main purpose is to defend data privacy, inter alia, by cybersecurity, data privacy and civil liberties are provided for in the specific laws mentioned already. Here telecommunications and telemedia shall serve as examples.

For the telecommunications sector the TKG rules that every service provider shall be obliged to maintain telecommunications privacy – also in relation to interception by means of radio equipment (ie, the content and detailed circumstances of telecommunications as well as the fact of whether or not a person is or was engaged in a telecommunications activity). On the other hand, providers of publicly available telecommunications services have to provide, at their own expense, technical facilities that allow implementation of telecommunications interception measures if provided for by law. The conditions according to which a service provider itself may collect and use customer data (ie, the data of the subscriber), traffic data (eg, a number or other identification of the lines in question or of the terminal, personal authorisation codes, location data, beginning and end of the connection, etc) or location data are laid down specifically in the TKG.

For telemedia services there are also certain provisions on data privacy for its users, but only insofar as these services are for private use. Similar to the provisions in the BDSG, collection and processing of personal data of these users is forbidden unless allowed by the TMG or any other legal provision that specifically refers to telemedia or with the user's consent.

Generally, the service provider has to secure by technical and organisational measures that:

- the user can end the use of the service anytime;
- the user can delete or block all personal data about the way of access or any other use immediately after the end of usage;
- the user can use telemedia in a way secure against access by a third party;
- personal data about the use of different telemedia by the same user can be used separately;
- certain data can only be unified for billing purposes; and
- usage profiles cannot be unified with information on the identification of the user of a pseudonym. The service provider has to enable the use of telemedia and its payment anonymously or pseudonomised, as far as technically possible and reasonable.

Similar to the provisions for telecommunications, the conditions according to which a service provider may collect, process or disclose personal data of the user as well as usage data is specifically regulated.

These provisions are accompanied by various mandatory notifications for users.

10 What are the principal cyberactivities that are criminalised by the law of your jurisdiction?

The main cybercrimes mentioned in the general Criminal Code are:

- data espionage: unlawfully obtaining data (stored or transmitted electronically or magnetically or otherwise in a manner not immediately perceivable) not intended for the culprit and especially protected against unauthorised access, by circumventing the protection – sentence: imprisonment not exceeding three years or a fine;
- phishing: intercepting data not intended for the culprit by technical means from a non-public data processing facility or from the electromagnetic broadcast of a data processing facility (even if not specifically protected) – sentence: imprisonment not exceeding two years or a fine, unless the offence incurs a more severe penalty under other provisions;
- acts preparatory to data espionage and phishing, such as preparing the commission of an offence mentioned above by producing, acquiring, selling, supplying to another, disseminating or making otherwise accessible passwords or other security codes enabling access to data or software for the purpose of the commission of such an offence (hacking tools) – sentence: imprisonment not exceeding one year or a fine;
- computer fraud: damaging the property of another by influencing the result of a data processing operation through incorrect configuration of a program, use of incorrect or incomplete data, unauthorised use of data or other unauthorised influence on the course of the processing with the intent of obtaining an unlawful material benefit – sentence: imprisonment not exceeding five years or a fine;
- the preparation of an offence mentioned above by writing computer programs the purpose of which is to commit such an act, procurement, offering for sale, holding or supplying them to another is considered a crime – sentence: imprisonment not exceeding three years or a fine;
- violation of postal and telecommunications confidentiality: unlawfully disclosing to another person facts that are subject to postal or telecommunications confidentiality and that became known to him or her as the owner or employee of an enterprise in the business of providing postal or telecommunications services – sentence: imprisonment not exceeding five years or a fine;
- data tampering: unlawfully deleting, suppressing, rendering unusable or altering data – sentence: imprisonment not exceeding two years or a fine;
- computer sabotage: interfering with data processing operations that are of substantial importance to another by data tampering, entering or transmitting data with the intention of causing damage to another or destroying, damaging, rendering unusable, removing or altering a data processing system or a data carrier – sentence: imprisonment not exceeding three years or a fine; in serious cases (eg, the data processing operation is of substantial importance for another's business, enterprise or a public authority), the penalty shall be imprisonment not exceeding five years or a fine; and in especially serious cases (ie, major financial loss, acting on a commercial basis or as a member of a gang whose purpose is the continued commission of computer sabotage or jeopardising the population's supply with vital goods or services or the national security of Germany) the penalty shall be imprisonment from six months to 10 years; and
- disruption of telecommunications facilities: preventing or endangering the operation of a telecommunications facility that serves public purposes by destroying, damaging, removing, altering or rendering unusable an object that serves its operation, or taps electrical power intended for its operation – sentence: imprisonment not exceeding five years or a fine.

In addition, there are further offences involving documents laid down in the Criminal Code that might be applicable in cases of cyberactivity, such as, for example, forgery of technical records, forgery of data intended to provide proof, meaning of deception in the context of data processing or suppression of documents.

In addition, in specific acts, further criminal sanctions are laid down, such as:

- section 148 TKG: intercepting a communication or imparting to others the content of a communication or the fact of its reception or owning or manufacturing, marketing, import or otherwise introducing in the area of application of the TKG transmitting equipment against the respective provisions laid down in the TKG – sentence: imprisonment not exceeding two years or a fine; and

- criminal use of personal data (section 44 BDSG): wilfully committing certain offences that are generally considered to be administrative offences but in exchange for payment or with the intention of enriching oneself or another person, or of harming another person – sentence: imprisonment for up to two years or a fine.

11 How has your jurisdiction addressed information security challenges associated with cloud computing?

From a data privacy point of view, cloud computing services are generally considered to be data processing services that need a processing agreement for which specific content is mandatory, including documentation of technical and organisational measures of the processor.

Apart from these legal provisions, the German Ministry for Economy and Energy (BMWi) started a technology competition called TrustedCloud in September 2010 as part of the ICT, which included 14 different projects, and the High Tech Strategy. It is aimed at the development and testing of innovative, secure and legal cloud computing solutions. Results can be found on http://trusted-cloud.de/798.php.

For the legal aspects of cloud computing a separate working group was formed in which experts from the economy, legal professions and science as well as representatives from Data Privacy Authorities together with members of the TrustedCloud program worked on solutions for legal challenges. The focus was on privacy, contract design, copyright as well as liability and criminal risks. In addition, there was a pilot project for a privacy certificate for cloud services. This working group published guidelines for each of these topics (see http://trusted-cloud.de/560.php).

The first certificate has been given to the General Association of the German Insurance Industry for its 'Trusted German Insurance Cloud' for providing secure services for the insurance sector.

There are further initiatives dealing with cloud services on various levels.

12 How do your jurisdiction's cybersecurity laws affect foreign organisations doing business in your jurisdiction? Are the regulatory obligations the same for foreign organisations?

There are no specific and separate provisions for foreign organisations. For each potentially relevant act it has to be checked if and under which circumstances this specific act is applicable. It may be, for example, related to the seat of the organisation or its branches or subsidiaries; it may also be related to the fact that services are offered or data stored within the geographic scope.

Best practice

13 Do the authorities recommend additional cybersecurity protections beyond what is mandated by law?

As mentioned above there are some more or less specific provisions in the binding laws on measures for cybersecurity. In addition there are sector-specific guidelines and recommendations. The most prominent recommendations or guidelines are the 'IT Basic Security Catalogues'. For details, see question 3. In addition, there are guidance documents, for example, for penetration testing, issued by the BSI.

14 How does the government incentivise organisations to improve their cybersecurity?

There is a government initiative called 'IT security in the economy'. It offers tools to evaluate the IT security level in companies, for example, an online IT security check.

Grants are generally paid for research projects, consulting services in the area of cybersecurity or specific measures for SME, for example, the German Federal Ministry of Education and Research has granted funding of around €120 million for its Research Agenda Industry 4.0, which includes funding for projects in IT security.

15 Identify and outline the main industry standards and codes of practice promoting cybersecurity. Where can these be accessed?

The main industry standard is ISO 27001: www.iso.org.

In addition, the 'Common Criteria for Information Technology Security Evaluation' is applied: www.commoncriteriaportal.org or www.bsi.bund.de/DE/Themen/ZertifizierungundAnerkennung/Produktzertifizierung/ZertifizierungnachCC/zertifizierungnachcc_node.html.

The IT Basic Security Catalogues of the BSI can be accessed in English at www.bsi.bund.de/EN/Publications/BSIStandards/BSIStandards_node.html.

The catalogue of security requirements for telecommunications service providers published by the Federal Regulation Authority can be accessed, only in German, at www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Anbieterpflichten/OeffentlicheSicherheit/KatalogSicherheitsanforderungen/KatalogSicherheitsanforderungen.pdf?__blob=publicationFile&v=2.

16 Are there generally recommended best practices and procedures for responding to breaches?

Many companies try to solve the issue internally. According to a recent study of corporate trust, only in a few cases (about 25 per cent) are external firms or public bodies consulted, mainly seeking advice in relation to eavesdropping. Only in less than 10 per cent of the cases have police, public prosecutors or offices for the protection of the constitution been contacted. Generally it seems most companies avoid interacting with authorities and the media unless legally required.

17 Describe practices and procedures for voluntary sharing of information about cyberthreats in your jurisdiction. Are there any legal or policy incentives?

There are several initiatives promoting voluntary information on cyberthreats. For example, the BSI offers a newsletter with up-to-date information on threats and preventive measures for the general public as well as to specialists. The Federal Association for Information Technology, Telecommunications and New Media also informs regularly about cyberthreats and preventive measures for industry as well as private persons.

18 How do the government and private sector cooperate to develop cybersecurity standards and procedures?

There are several initiatives for cooperation between government and the private sector, for example:

- Alliance for cybersecurity: an initiative of the BSI founded in cooperation with the Federal Association for Information Technology, Telecommunications and New Media. It is an alliance of important entities in the area of cybersecurity in Germany with the aim of providing up-to-date and valid information, a knowledge base and exchange of information and experience (see www.allianz-fuer-cybersicherheit.de);
- UP KRITIS: a public-private partnership for the protection of critical infrastructure (with the exception of state and administration). Participants are organisations with seats in Germany that operate critical infrastructure, professional and sector associations from the KRITIS-sectors as well as the competent authorities. Its aims are:
  - promotion of robust critical processes;
  - interchange on current incidents;
  - joint assessment and evaluation of risks, dependencies and the cybersecurity situation;
  - development of joint documents and positions;
  - development and expansion of crisis management structures;
  - coordinated crisis reaction and capacity;
  - execution of emergency and crisis training; and
  - joint action towards third parties (further information is available on www.upkritis.de and www.kritis.bund.de);
- TeleTrusT – Bundesverband IT-Sicherheit eV (Federal Association of IT Security): a competence network including domestic and foreign members from industry, administration and science as well as partner organisations dealing with similar topics. The aim of the association is the promotion of the reliability of IT and communications techniques. Its members include many big IT companies, authorities, public institutions including several Fraunhofer institutes, insurance associations, the BSI, Federal Criminal Police as well as many small or medium-sized companies and associated groups such as the Federal Association of German Banks, eco (the Association of the German Internet Industry), davit (the German Lawyers Association with is working group IT-Law), as well foreign associations such as the FNTC (France), EEMA (UK), AUSTRIAPRO (Austria), ISSS (Switzerland), ESRA (US), GABA (US) and the German Asia-Pacific Business Association (OAV); and

- DCSO (German Cyber Security Organisation): a group founded by the four DAX-groups Volkswagen, Allianz, BASF and Bayer. It serves as competence centre and cybersecurity service provider for the German economy as well as an interface to the federal institutions.

19 Is insurance for cybersecurity breaches available in the jurisdiction and is such insurance common?

Many insurance companies offer specific IT policies, which offer insurance against, for example, hacker attacks, theft and destruction of data, interruption of business or claims by third parties due to cyberattacks. For companies whose business model relies on the internet or for big industry groups such insurance is rather common nowadays. In mid-2014 it was announced that Bosch had allegedly insured the company against cybercrime for an amount of up to €100 million per attack. For SMEs the issue is not yet a primary focus. According to a recent study by Corporate Trust, only 3.6 per cent of companies in Germany have such insurance, 24 per cent think about it, but 92.5 per cent of the companies surveyed declared themselves willing to only pay much less than €100,000 for it.

Enforcement

20 Which regulatory authorities are primarily responsible for enforcing cybersecurity rules?

The main authorities responsible for enforcing cybersecurity rules are the following:

- the BSI, responsible for ensuring the security of federal information technology and responsible for operators of critical infrastructure;
- the Federal Regulatory Authority, responsible for telecommunication service providers;
- the Federal Commissioner for Data Protection and Freedom of Information, responsible for monitoring compliance by the federal public bodies with the provisions of the BDSG and other data protection provisions;
- the 16 state officers for data protection, responsible for monitoring compliance with data protection provisions by the public bodies of the respective state as well as for the private sector; and
- the main police, the public prosecutors, the BKA or state offices for criminal investigations are mainly in charge of prosecuting cybercrimes.

21 Describe the authorities' powers to monitor compliance, conduct investigations and prosecute infringements.

Within the telecommunications sector the Federal Regulatory Authority can, inter alia, order that service providers are reviewed by an independent party. It may give other orders and take other measures to secure compliance with the TKG, ordinances and applicable technical directives. It is authorised to enter and inspect business premises and production sites and to ask for information. It has similar investigation rights as public attorneys (ie, hear witnesses, confiscate evidence, take provisional measures). The Regulatory Authority may also impose administrative sanctions.

The BSI can review audit and other internal investigation results, can ask for remediation of security failings and may set requirements for security audits, checks and certificates as well as for measures.

There are similar monitoring and investigation rights to those of the other supervisory authorities mentioned in question 20.

22 What are the most common enforcement issues and how have regulators and the private sector addressed them?

In Germany the BSI supports industry in identifying attacks and informing about protection methods rather than sentencing industry in the case of identified leakages (unless identified issues are not remedied). Nevertheless, the BSI and the Federal Criminal Police investigate in cases of cybersecurity threats.

The following proposals aim at increasing protection against cyberattacks:

- there is the possibility of anonymously notifying incidents that may have an impact on others. This aims at gaining knowledge about new attack methods or critical incidents also in cases where there is no obligation to notify. So far mainly SMEs report such incidents;
- there are initiatives to foster standards like 'made in Germany' such as 'e-mail made in Germany' or, for example, the SINA product family (designed and promoted by the BSI) by which IT-supported 'secure workplaces' are provided, which enables use of application product lines of the market leaders without risk; and
- there is a willingness to engage in standardisation and certification, for example, for the standard OPC UA (the central protocol in connection with industry 4.0).

23 What penalties may be imposed for failure to comply with regulations aimed at preventing cybersecurity breaches?

For critical infrastructure, penalties of up to €50,000 can be set for not implementing security measures and in the case of non-adherence to a specific order the fine can rise to €100,000.

In the telecommunications sector the Federal Regulatory Authority can set penalty payments. Depending on the underlying offence they may range up to €20,000 or €500,000. In the case of repeated violations, services can be restricted in such a way that the customer base can be frozen until the violation is remedied (except expiration of a contract or termination). It may even prohibit the operation of the telecommunication system or all or part of the provision of the services, if less severe means are insufficient.

In the telemedia sector the Authority may impose administrative fines of up to €50,000 in the case of violation of certain duties related to provisions applicable to private users pursuant to the TMG.

The data protection authorities can prohibit single processes with which personal data are collected, processed or used in the case violations are not remedied in due time. They can also set fines, depending on the underlying offence of up to €50,000 or €300,000. These fines are mainly related to violations of data privacy rather than to cybersecurity.

24 What penalties may be imposed for failure to comply with the rules on reporting threats and breaches?

In the telecommunications sector, penalties for failure to comply with reporting duties may be punished by fines of up to €50,000 or €100,000, depending on the offence, and in serious cases up to €500,000. Failure to report a threat in the sector of critical infrastructure may be punished with a fine of up to €50,000. A breach of reports due according to the BDSG can be punished with a fine of up to €300,000.

25 How can parties seek private redress for unauthorised cyberactivity or failure to adequately protect systems and data?

Parties affected by a security breach mainly have rights to be informed and may have claims for damages against companies, service providers and the like who fail to adequately protect their systems. Unless there are specific regulations on how to protect the systems there might be practical problems to prove intentional or negligent act or omission.

Companies that have suffered damages from cyberactivity by individuals (intentionally, negligently or even without the individual's knowledge) may have claims for damages pursuant general liability provisions. In many cases these claims suffer from the inability to ascertain the culprit's identity and to demonstrate the damage.

Questions about the duties of care single (especially private) users might have to protect their own systems against attacks or against being misused by third parties for cyberattacks have not yet been legally answered.

Threat detection and reporting

26 What policies or procedures must organisations have in place to protect data or information technology systems from cyberthreats?

As mentioned above, in many provisions there is no specific provision on how systems have to be protected against cyberthreats. In many cases such specification is laid down either in technical provisions (in most cases non-binding) or recommendations. The BDSG, for example, specifically states in its Annex (in which the technical and organisational measures are listed) that state-of-the art encryption measures can be considered as means to prevent data processing systems from being used without authorisation, to ensure that persons authorised to use a data processing system have access only to those data they are authorised to access, and that personal data cannot be read, copied, altered or removed without authorisation during processing, use and after recording access control, disclosure control, and to ensure that personal data cannot be read, copied, altered or removed without authorisation during electronic transfer or transport or while being recorded onto data storage media. As of July 2014 encryption is also

mentioned as a means to secure a telemedia service provider's IT system in the TMG.

27 Describe any rules requiring organisations to keep records of cyberthreats or attacks.

There are no specific rules that oblige organisations to keep such records.

28 Describe any rules requiring organisations to report cybersecurity breaches to regulatory authorities.

According to the new provisions in the BSIG, operators of critical infrastructure have to immediately notify severe disruptions of availability, integrity, authenticity and confidentiality of their IT systems, components or processes, which either led or could lead to an outage or impairment of the critical infrastructure to the BSI. The notice can be made anonymously unless there was actually an outage or impairment.

In the telecommunications sector a service provider has to notify the Federal Regulatory Authority of any breach of security including disruption of telecommunication networks or services without delay, insofar as considerable effects result thereof for the operation of these networks or services. Cases of personal data breach must also be reported to the Authority as well as to Federal Data Protection Commissioner, unless it can be proven by the security plan that the respective personal data have been secured by appropriate technical means, specifically by using an encryption method generally recognised as safe. The service provider has to describe the consequences of the personal data breach as well as the measures planned and taken.

In the telemedia sector an information duty applies where a service provider recognises that user or usage data stored by it has been unlawfully transferred or accessed, threatening serious harm to the rights or legitimate interests of data subjects. The notification duties according to section 42a BDSG apply.

Section 42a BDSG states that where the controller determines that (i) sensitive data, (ii) personal data subject to professional secrecy, (iii) personal data referring to (suspected) criminal or administrative offences, or (iv) personal data concerning bank or credit card accounts have been unlawfully transferred or otherwise unlawfully disclosed to third parties, threatening serious harm to the rights or legitimate interests of data subjects, the controller has to notify the competent supervisory authority without delay, including possible harmful consequences of the unlawful disclosure and measures taken by the body as a result.

29 What is the timeline for reporting to the authorities?

Notifications to authorities have to take place only in the case of a specific incident. For the timeline, see question 28.

Update and trends

As mentioned in this chapter, the main change to cybersecurity laws in Germany in 2015 has been the new IT Security Act, which changed the BSI Act and several other provisions. However, important details are still to be defined in a separate ordinance. This includes the scope of operators of critical infrastructure as well as details on the organisational and technical security measures. In addition, the planned EU Regulation on Privacy foresees increased reporting duties to authorities. Therefore, many details of future legal requirements are currently unknown.

In the security report of the BSI for 2015, the following developments have been highlighted as critical. Due to the rising amount of known vulnerabilities, some IT manufacturers tend not to provide security updates for less critical security gaps. Attacks against industrial production sites have risen. And, in the course of digitalising, aspects of IT security are often not sufficiently considered. From a technical point of view the increasing trend to software-defined solutions, mobile computing and compatibility of systems on the one hand and the decision on software on the other form increasing risks for cybersecurity.

In order to accompany the development of digitalising, the German federal government has developed a 'Digital Agenda 2014 – 2017'. It is aimed at the main topics, one of which is increasing the security of IT systems and services.

30 Describe any rules requiring organisations to report threats or breaches to others in the industry, to customers or to the general public.

According to section 42a BDSG, data subjects shall be informed as soon as appropriate measures to safeguard the data have been taken and notification would no longer endanger criminal prosecution. The notification shall describe the nature of the unlawful disclosure and recommend measures to minimise possible harm. Where notifying the data subjects would require a disproportionate effort, in particular due to the large number of persons affected, such notification may be replaced by public advertisements of at least one-half page in at least two national daily newspapers, or by another equally effective measure for notifying data subjects.

In the telecommunications sector, the Federal Regulatory Authority can decide in the case of security incidents to inform the general public or ask the service provider to do so if it concludes that the information is in the general interest. In the case of a personal data breach the service provider has to inform the persons affected without delay, if it has to be assumed that the users or other persons have been seriously affected by the breach. The content of the notice is similar to the one mentioned above.

ARNDT
Rechtsanwaltsgesellschaft mbH

Svenja Arndt **s.arndt@arndt-ra.de**

Poßbergweg 3
40629 Düsseldorf
Germany

Tel: +49 211 94211 556
Fax: +49 211 94211 558
www.arndt-ra.de

India

Salman Waris

TechLegis, Advocates & Solicitors

Legal framework

1 Summarise the main statutes and regulations that promote cybersecurity. Does your jurisdiction have dedicated cybersecurity laws?

India does not have dedicated cyberlaws for the promotion of cybersecurity. However, the cybersecurity regulations are enshrined under the Information Technology Act, 2000 as amended from time to time (IT Act).

The IT Act and the rules framed under it embody the principles and rules governing cybersecurity. The following rules under the IT Act have a bearing on cybersecurity:

- the Information Technology (Security Procedure) Rules, 2004;
- the Information Technology (Procedure and safeguards for interception, monitoring and decryption of information) Rules, 2009;
- the Information Technology (Procedure and safeguards for blocking for access of information by public) Rules, 2009;
- the Information Technology (Procedure and safeguard for monitoring and collecting traffic data or information) Rules, 2009;
- the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011;
- the Information Technology (Intermediaries guidelines) Rules, 2011;
- the Information Technology (Guidelines for Cyber Cafe) Rules, 2011;
- the Information Technology (Electronic Services Delivery) Rules, 2011; and
- the National Cyber Security Policy, 2013.

2 Which sectors of the economy are most affected by cybersecurity laws and regulations in your jurisdiction?

The industry sectors most affected by the cybersecurity laws and regulation in India are information technology (IT), information technology enabled services, software and services, banking, e-commerce, health care including telemedicine and mobile clinics, financial services including mobile banking and payment gateways, and social media. These sectors are directly affected by acts concerning cyberlaws and security.

There have been drastic steps initiated towards the implementation of cybersecurity for these activities, such as implementation of secure payment gateways, use of secure encryption standards, etc. The Reserve Bank of India and the Securities and Exchange Board of India have prescribed standards for secure financial transactions in the country.

3 Has your jurisdiction adopted any international standards related to cybersecurity?

International standards pertaining to cybersecurity have been incorporated and prescribed under the IT Act and the rules thereunder.

In this regard, the International Standard ISO/IEC 27001 on 'Information Technology – Security Techniques – Information Security Management System – Requirements' has been prescribed by rule 8 of the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 for security practices and procedures.

4 What are the obligations of responsible personnel and directors to keep informed about the adequacy of the organisation's protection of networks and data, and how may they be held responsible for inadequate cybersecurity?

Responsibility of the personnel and directors of a company has been set out in provisions of section 85 of the IT Act, where such company acts in violation of the provisions of the IT Act or the rules thereunder.

At the time the contravention was committed, every person who was in charge of and was responsible for the conduct of business of the company, as well as the company, shall be guilty of the contravention and shall be liable to be proceeded against and punished accordingly.

Where a contravention of any of the provisions of the IT Act or of any rule, direction or order made thereunder has been committed by a company and it is proven that the contravention has taken place with the consent or connivance of, or is attributable to any neglect on the part of, any director, manager, secretary or other officer of the company, such director, manager, secretary or other officer shall also be deemed to be guilty of the contravention and shall be liable to be proceeded against and punished accordingly.

5 How does your jurisdiction define cybersecurity and cybercrime?

'Cybersecurity' has been defined under section 2(nb) of the IT Act and means protecting information, equipment, devices, computers, computer resources, communication devices and information stored therein from unauthorised access, use, disclosure, disruption, modification or destruction.

'Cyber incidents' have been defined under rule 2(d) of the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 as any real or suspected adverse event in relation to cybersecurity that violates an explicitly or implicitly applicable security policy resulting in unauthorised access, denial of service or disruption, unauthorised use of a computer resource or processing or storage of information or changes to data or information without authorisation.

6 What are the minimum protective measures that organisations must implement to protect data and information technology systems from cyberthreats?

The Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 impose strict conditions for the collection, transfer and disclosure of 'sensitive personal data or information'. The Rules also prescribe the situations and modes wherein 'sensitive personal data or information' can be collected, transferred or disclosed. Conditions such as prior consent, collection and use for a lawful purpose or activity and retention, disclosure and transfer only to such extent as required have been imposed with regard to the data falling within the category of 'sensitive personal data or information'. Any body corporate handling sensitive personal data or information is obligated to implement and maintain reasonable security practices and procedures.

The IT Act defines an 'intermediary' under section 2, as any person, with respect to any particular electronic record, who on behalf of another person receives, stores or transmits that record or provides any service with respect to that record. An intermediary includes telecoms service providers, network service providers, internet service providers, web-hosting service providers, search engines, online payment sites, online auction sites, online marketplaces and cybercafes, etc.

Additionally, the Information Technology (Intermediaries Guidelines) Rules, 2011 stipulates that all entities covered within the definition of intermediary and performing functions thereof are obligated to observe due diligence while discharging its duties as an intermediary.

7 Does your jurisdiction have any laws or regulations that specifically address cyberthreats to intellectual property?

There are no specific regulations concerning cyberthreats to intellectual property. However, the Trade Marks Act, 1999 provides for protection against the infringement of trademarks and the Copyrights Act, 1957 provides for protection against the infringement of copyright. The said legislation generally covers and protects against all acts of infringement. The Indian courts have judicially extended the principles of the legislation to include infringement that occurs in the cyberworld as well.

The Information Technology (Intermediaries Guidelines) Rules, 2011 provides that the intermediaries, as defined under the IT Act, are required to ensure they do not host, display, upload, modify, publish, transmit, update or share any information that infringes any patent, trademark, copyright or other proprietary rights.

8 Does your jurisdiction have any laws or regulations that specifically address cyberthreats to critical infrastructure or specific sectors?

The Information Technology (National critical information infrastructure protection centre and manner of performing functions and duties) Rules, 2013, issued on 16 January 2014 under the provisions of section 70A of the IT Act, specifically deals with the critical information infrastructure.

'Critical information infrastructure' has been defined by the IT Act as such computer resource, the incapacitation or destruction of which, shall have a debilitating impact on national security, economy, public health or safety.

9 Does your jurisdiction have any cybersecurity laws or regulations that specifically restrict sharing of cyberthreat information?

While there is no specific law restricting the sharing of cyberthreat information there is, however, section 66 E of the amended IT Act, which deals with issues relating to violation of privacy, which may be interpreted to cover the issue of recording or accessing private communication, an act that may be interpreted as a punishable offence.

Besides, where a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource that it owns, controls or operates is negligent in implementing and maintaining reasonable security practices and procedures and, thereby, causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation to the person so affected.

Additionally, any person who is required under the IT Act to:

- furnish any document, return or report to the controller or the certifying authority fails to furnish the same, shall be liable to a penalty not exceeding 150,000 rupees for each such failure;
- file any return or furnish any information, books or other documents within the time specified therefor in the regulations fails to file a return or furnish the same within the time specified therefor in the regulations, shall be liable to a penalty not exceeding 5,000 rupees for every day during which such failure continues; and
- maintain books of account or records fails to maintain the same, shall be liable to a penalty not exceeding 10,000 rupees for every day during which the failure continues.

The IT Act also provides for a residuary penalty, which states that for the contravention of which no penalty has been separately provided, a person shall be liable to pay compensation not exceeding 25,000 rupees to the person affected by such contravention.

10 What are the principal cyberactivities that are criminalised by the law of your jurisdiction?

With regard to the criminalisation of cyberactivities and offences, the IT Act provides for the following offences and punishments:

- tampering with computer source documents: punishable by imprisonment of up to three years, or a fine of up to 200,000 rupees, or both;
- computer-related offences: the IT Act provides that where any person commits the following acts, they shall be liable to pay damages as compensation to the person so affected. Further, if such act is carried on by the person dishonestly or fraudulently, such person shall be punishable by imprisonment for a term of up to three years or a fine of up to 500,000 rupees, or both:
  - accesses or secures access to such computer, computer system or computer network;
  - downloads, copies or extracts any data, computer database or information from such computer, computer system or computer network including information or data held or stored in any removable storage medium;
  - introduces or causes to be introduced any computer contaminant or computer virus into any computer, computer system or computer network;
  - damages or causes to be damaged any computer, computer system or computer network, data, computer database or any other programs residing in such computer, computer system or computer network;
  - disrupts or causes disruption of any computer, computer system or computer network;
  - denies or causes the denial of access to any person authorised to access any computer, computer system or computer network by any means;
  - provides any assistance to any person to facilitate access to a computer, computer system or computer network in contravention of the provisions of this Act, rules or regulations made thereunder;
  - charges the services availed of by a person to the account of another person by tampering with or manipulating any computer, computer system, or computer network;
  - destroys, deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means; or
  - steals, conceals, destroys or alters or causes any person to steal, conceal, destroy or alter any computer source code used for a computer resource with an intention to cause damage;
- sending offensive messages through a communication service that is grossly offensive or has menacing character or is for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred or ill will: punishable by imprisonment of up to three years and a fine;
- dishonestly receiving stolen computer resources or communication devices: punishable by imprisonment of up to three years or a fine of up to 100,000 rupees, or both;
- identity theft: punishable by imprisonment of of up to three years and a fine of up to 100,000 rupees;
- cheating by impersonation by using a computer resource: punishable by imprisonment of up to three years and a fine of up to 100,000 rupees;
- violation of privacy: punishable by imprisonment of up to three years or a fine of up to 200,000 rupees, or both;
- cyberterrorism: punishable by imprisonment, which may extend to imprisonment for life;
- publishing or transmitting obscene material in electronic form: punishable, on first conviction, by imprisonment of up to three years and a fine of up to 500,000 rupees, and in the event of a second or subsequent conviction by imprisonment of up to five years and a fine of up to 1 million rupees;
- publishing or transmitting of material containing sexually explicit acts, etc, in electronic form: punishable, on first conviction, by imprisonment of up to five years and a fine of up to 1 million rupees, and in the event of a second or subsequent conviction by imprisonment of up to seven years and a fine of up to 1 million rupees;
- publishing or transmitting of material depicting children in sexually explicit acts, etc, in electronic form: punishable, on first conviction, by imprisonment of up to five years and fine of up to 1 million rupees, and in the event of a second or subsequent conviction by imprisonment of up to to seven years and a fine of up to 1 million rupees;

- preservation and retention of information by intermediaries for a duration not in line with the manner and format as prescribed by the government: punishable by imprisonment of up to three years and a fine;
- non-compliance with any order of the controller: punishable by imprisonment of up to two years or a fine of up to 100,000 rupees, or both;
- non-compliance with directions for interception or monitoring or decryption of any information through any computer resource: punishable by imprisonment of up to seven years and a fine;
- non-compliance with directions for blocking public access to any information through any computer resource by an intermediary: punishable by imprisonment of up to seven years and a fine;
- not providing support for monitoring and collection traffic data or information through any computer resource for cybersecurity: punishable by imprisonment of up to three years and a fine;
- securing access or attempting to secure access to a protected system, as declared by the government: punishable by imprisonment of up to 10 years and a fine;
- failure to provide the information called for or failure to comply with the directions of the Computer Emergency Response Team: punishable by imprisonment of up to one year or a fine of up to 100,000 rupees, or both;
- misrepresentation or suppressesion of any material fact from the controller or the certifying authority for obtaining any licence or electronic signature certificate: punishable by imprisonment of up to two years, or a fine of up to 100,000 rupees, or both;
- breach of confidentiality and privacy: punishable by imprisonment of up to two years, or a fine of up to 100,000 rupees, or both;
- disclosure of information in breach of lawful contract: punishable by imprisonment of up to three years, or a fine of up to 500,000 rupees, or both;
- publishing false electronic signatures in certain particulars: punishable by imprisonment of up to two years, or a fine of up to 100,000 rupees, or both;
- publication for fraudulent or unlawful purpose: punishable by imprisonment of up to two years, or a fine of up to 100,000 rupees, or both; and
- confiscation: any computer, computer system, floppies, compact disks, tape drives or any other accessories related thereto, in respect of which any provision of this Act, rules, orders or regulations made thereunder has been or is being contravened, shall be liable to confiscation:

Further, it is provided that no compensation awarded, penalty imposed or confiscation made under this Act shall prevent the award of compensation or imposition of any other penalty or punishment under any other law currently in force.

11 How has your jurisdiction addressed information security challenges associated with cloud computing?

At present there are no specific legislative or regulatory measures implemented to addressed information security challenges associated with cloud computing. Issues relating to cloud computing and associated information security challenges are currently dealt with contractually between parties who may impose internationally applicable standards or measures.

12 How do your jurisdiction's cybersecurity laws affect foreign organisations doing business in your jurisdiction? Are the regulatory obligations the same for foreign organisations?

The IT Act has been made applicable to any offence or contravention committed outside India by any person irrespective of his or her nationality. Section 75 of the IT Act provides that this Act shall apply to an offence or contravention committed outside India by any person if the act or conduct constituting the offence or contravention involves a computer, computer system or computer network located in India.

Best practice

13 Do the authorities recommend additional cybersecurity protections beyond what is mandated by law?

The authorities have not recommended additional norms and practices and primarily enforce the provisions mandated by the IT Act and the rules made thereunder. However, certain self-regulatory bodies have issued regulatory frameworks and best practices for their member entities. The Data Security Council of India (DSCI) has published the DSCI Privacy Best Practices and the DSCI Security Framework, which would be applicable to its members.

14 How does the government incentivise organisations to improve their cybersecurity?

At present, no provision for such incentives has been initiated through the existing legislation.

15 Identify and outline the main industry standards and codes of practice promoting cybersecurity. Where can these be accessed?

The primary rules for cybersecurity are enshrined in the IT Act and the rules made thereunder. The International Standard ISO/IEC 27001 on 'Information Technology – Security Techniques – Information Security Management System – Requirements' has been prescribed by rule 8 of the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 for the security practices and procedures.

16 Are there generally recommended best practices and procedures for responding to breaches?

There have been instances where various self-regulatory organisations have laid down best practices and procedures for responding to breaches of cybersecurity by the DSCI. The DSCI has issued the DSCI Privacy Best Practices and the DSCI Security Framework, which would be applicable to its members.

17 Describe practices and procedures for voluntary sharing of information about cyberthreats in your jurisdiction. Are there any legal or policy incentives?

The sharing of information about cyberthreats has been discussed above.

18 How do the government and private sector cooperate to develop cybersecurity standards and procedures?

The cooperation between the government and the private sector is stipulated in terms of the formulation of the reasonable security practices and procedures. The IT Act under the provisions of section 43A obligates a body corporate handling sensitive personal data or information to implement and maintain reasonable security practices and procedures. These 'reasonable security practices and procedures' mean security practices and procedures designed to protect such information from unauthorised access, damage, use, modification, disclosure or impairment, as may be specified in an agreement between the parties or as may be specified in any law currently in force and in the absence of such agreement or any law, such reasonable security practices and procedures as may be prescribed by the government in consultation with such professional bodies or associations as it may deem fit.

19 Is insurance for cybersecurity breaches available in the jurisdiction and is such insurance common?

Cyber liability insurance is generally regarded as an extension to professional indemnity policy. Such policies cover computer virus, misrepresentation, defamation, confidentiality breach, intellectual property infringement and other related risks. However, such provisions are not universally applicable and the term of policy should be considered before relying on such policies in an absolute manner.

Enforcement

20 Which regulatory authorities are primarily responsible for enforcing cybersecurity rules?

The regulatory bodies responsible for enforcing cybersecurity rules comprise the following:

- the Indian Computer Emergency Response Team (CERT-In) and the sectoral CERTs;
- the Department of Information Technology;
- the Department of Telecommunications;
- the Ministry of Home Affairs;
- the Ministry of Defence;
- the National Information Board;

- the National Crisis management Committee;
- the National Security Council Secretariat;
- the National Information Infrastructure Protection Centre;
- the National Disaster Management Authority of India; and
- the Standardisation, Testing and Quality Certification Directorate.

21 Describe the authorities' powers to monitor compliance, conduct investigations and prosecute infringements.

The regulatory authorities dealing with cybersecurity investigations are as follows:

- the CERT-In monitors Indian cyberspace and coordinates alerts and warnings of imminent attacks and detection of malicious attacks among public and private cyber users and organisations in the country;
- the National Information Infrastructure Protection Centre is a designated agency to protect the critical information infrastructure in the country. It gathers intelligence and keeps a watch on emerging and imminent cyberthreats in strategic sectors including national defence;
- the Department of Information Technology (DIT) is under the Ministry of Communications and Information Technology, government of India. The DIT strives to make India a global leading player in information technology and at the same time take the benefits of IT to every walk of life in order to develop an empowered and inclusive society. It is mandated with the task of dealing with all issues related to promotion and policies in electronics and IT;
- the Department of Telecommunications, under the Ministry of Communications and Information Technology, government of India, is responsible for coordinating with all ISPs and service providers with respect to cybersecurity incidents and response actions as deemed necessary by CERT-In and other government agencies;
- the National Information Board (NIB) is an apex agency with representatives from relevant departments and agencies that form part of the critical minimum information infrastructure in the country;
- the National Crisis Management Committee is an apex body of the government of India for dealing with major crisis incidents that have serious or national ramifications;
- the National Security Council Secretariat is an apex agency looking into the political, economic, energy and strategic security concerns of India and acts as the secretariat to the NIB;
- the Ministry of Home Affairs (MHA) issues security guidelines from time to time to secure physical infrastructure. The MHA sensitises the administrative departments and organisations about vulnerabilities and also assists the respective administrative ministry and departments;
- the Ministry of Defence (MoD) is the nodal agency for cybersecurity incident response with respect to defence sector. The MoD, Integrated Defence Staff (IDS), formed under the aegis of Headquarters IDS, is the nodal tri-services agency at the national level to effectively deal with all aspects of information assurance and operations;

Update and trends

In September 2015, a draft Encryption Policy formulated by an expert group set up by the Department of Electronics and Information Technology under section 84A of the Information Technology Act, 2000 was issued. The draft, which was applicable to everyone including government departments, academic institutions and citizens for all kinds of communications, proposed legal action that could entail imprisonment for failure to store and produce on demand the encrypted message from any mobile device or computer. However, after much criticism the government withdrew the draft and is reworking it.

- the National Disaster Management Authority is the apex body for disaster management in India and is responsible for the creation of an enabling environment for institutional mechanisms at the state and district levels; and
- the Standardisation, Testing and Quality Certification (STQC) Directorate is a part of the DIT and is an internationally recognised assurance service providing organisation. The STQC has established a nationwide infrastructure and developed competence to provide quality assurance and conformity assessment services in IT.

22 What are the most common enforcement issues and how have regulators and the private sector addressed them?

Some enforcement issues faced by the regulatory bodies in India are as follows:

- there is no territorial boundary and thus the jurisdiction issue arises when international breaches occur;
- technical complexities;
- law enforcement officials lack proper training in cyberlaws;
- anonymity over the internet and multiple protective layers instated by criminals are sometimes very hard to break and thus enforcement is negated; and
- the lack of proper user logs and lack of proper tools to monitor internet traffic.

23 What penalties may be imposed for failure to comply with regulations aimed at preventing cybersecurity breaches?

A list of the penalties set out under the IT Act has been segregated into civil liabilities and criminal penalties in questions 9 and 10 respectively. The same would be imposed for the relevant threats and breaches. In addition to the specific liabilities and penalties, the IT Act also provides for a residuary penalty, which states that for the contravention of which no penalty has been separately provided, a person shall be liable to pay compensation not exceeding 25,000 rupees to the person affected by such contravention.

Salman Waris **salman.waris@techlegis.com**

Level 1 Redfort Capital Parsavnath Towers
Bhai Veer Singh Marg
Gole Market, Connaught Place
New Delhi 110001
India

Tel: +91 98 9142 7685
Fax: +91 11 2636 0037
www.techlegis.com

24 What penalties may be imposed for failure to comply with the rules on reporting threats and breaches?

See questions 9, 10 and 22.

25 How can parties seek private redress for unauthorised cyberactivity or failure to adequately protect systems and data?

The parties are at liberty to seek private redress. The parties may either mutually negotiate and settle the matter or are also entitled to initiate arbitration proceedings under the provisions of and as prescribed by the Arbitration and Conciliation Act, 1996.

Threat detection and reporting

26 What policies or procedures must organisations have in place to protect data or information technology systems from cyberthreats?

To ensure protection from cyberthreats, a body corporate handling sensitive personal data or information is obligated to implement reasonable security practices and procedures. The body corporate is bound to adhere to the strict conditions for the collection, transfer and disclosure of the sensitive personal data or information, in order to ensure data protection.

Additionally, in terms of the Information Technology (Intermediaries Guidelines) Rules, 2011, the intermediary is also under an obligation not to host, display, upload, modify, publish, transmit, update or share any information that contains software viruses or any other computer codes, files or programs designed to interrupt, destroy or limit the functionality of any computer resource.

27 Describe any rules requiring organisations to keep records of cyberthreats or attacks.

There is no explicit requirement to keep a record of cyberthreats or breaches. However, the same is implicit in the manner that the cybersecurity incidents are to be reported to CERT-In by individuals, organisations or corporate entities.

28 Describe any rules requiring organisations to report cybersecurity breaches to regulatory authorities.

Cybersecurity incidents are to be reported to CERT-In by individuals, organisations or corporate entities.

29 What is the timeline for reporting to the authorities?

Pursuant to the Information Technology (the Indian Computer Emergency Response Team and manner of performing functions and duties) Rules, 2013, individuals, organisations or corporate entities, as the case may be, are required to report cybersecurity incidents to CERT-In within a reasonable time of the occurrence or of becoming aware of the incident.

30 Describe any rules requiring organisations to report threats or breaches to others in the industry, to customers or to the general public.

Individuals, organisations or corporate entities, as the case may be, are required to report incidents of cybersecurity breach to CERT-In, however, the obligation to report to the public is not a provision of the IT Act. Nevertheless, CERT-In, under the Information Technology (the Indian Computer Emergency Response Team and manner of performing functions and duties) Rules, 2013, has been assigned the function of publishing alerts and offering information for the improvement of cybersecurity.

Japan

Masaya Hirano and Kazuyasu Shiraishi
TMI Associates

Legal framework

1 Summarise the main statutes and regulations that promote cybersecurity. Does your jurisdiction have dedicated cybersecurity laws?

Japan has a dedicated cybersecurity law called the Basic Cybersecurity Act, which was enacted on 6 November 2014 (and promulgated on 12 November 2014). The Basic Cybersecurity Act is the first cybersecurity-specific law that has been enacted among the G7 nations.

The primary task of the Basic Cybersecurity Act is to ensure cybersecurity, while also ensuring free distribution of information. It is the purpose of the Basic Cybersecurity Act to move cybersecurity-related policies forward in a comprehensive and effective manner, and contribute to the creation of a more energetic and continuously developing economic society consequently contributing to the national security of Japan.

The Basic Cybersecurity Act is, as it sounds, basic law. In the future the government will develop more specific relevant laws and regulations on the basis of the Basic Cybersecurity Act.

At present, Japan has other substantive laws that include cybercrime such as the Penal Code, the Unfair Competition Prevention Act, the Unauthorised Computer Access Prohibition Act, the Instalment Sales Act, and the Specially Designated Secret Protection Act. In addition to cybercrime legislation, the Personal Information Protection Act was enacted in 2003 to protect personal information and identity. Further, the Social Security and Tax Number Act was enacted in 2013.

The Personal Information Protection Act relates to information security, but more specifically to the proper handling of personal information, rather than to cybersecurity per se. Although the Personal Information Protection Act prescribes concrete duties of a business operator handling personal information as prescribed in article 2, paragraph 3 of the said Act (personal information handling business operator), it does not prescribe concrete duties of administrative organs, independent administrative agencies and local governments. Concrete duties of administrative organs are prescribed in the Act on the Protection of Personal Information Held by Administrative Organs; those of independent administrative agencies are prescribed in the Act on the Protection of Personal Information Held by Independent Administrative Agencies, etc., and those of local governments are prescribed in privacy protection ordinances enacted by each local government.

The Personal Information Protection Act was amended in September 2015 (Amended Personal Information Protection Act) and is likely to become fully effective sometime before September 2017. The principal amendments made therein are as outlined below:

- clarification of the definition of 'personal information' (ie, elimination of grey areas and addition of new provisions concerning sensitive information);
- new provisions concerning the use of information anonymised pursuant to the method prescribed in the rules established by the Personal Information Protection Commission;
- new provisions concerning the traceability of personal information by the relevant individual identified by such personal information;
- new provisions concerning criminal penalties imposed in the event of personal information having been provided to obtain illicit gains;
- establishment of the Personal Information Protection Commission as an authority independent of other administrative organs, which will coordinate personal information protection policies in a unified manner; and
- provisions concerning overseas transfers of personal information and extraterritorial applicability of the Personal Information Protection Act of Japan.

2 Which sectors of the economy are most affected by cybersecurity laws and regulations in your jurisdiction?

The Basic Cybersecurity Act specifically prescribes, in addition to the cybersecurity duties of the state and the local authorities, the cybersecurity duties of critical infrastructure business operators (ie, those engaged in business pertaining to such infrastructure that forms the basis of the lives of Japanese nationals and economic activities and that is likely to have a considerable impact thereon in the event of any discontinuance or decrease of its functions), cyber-related business operators, universities and other educational or research institutions in the economic field. There is a possibility that in the future, duties for these business operators may be prescribed in further detail by more specific laws likely to be developed.

Revisions are currently being made to expand the scope for critical infrastructure business operators. In Japan, critical infrastructure business operators belonging to the following 10 sectors have conventionally been expected to safeguard the information with the same level of security as the governmental institutions are required to do. These sectors are:

- information and communications technologies (ICT);
- finance;
- aviation;
- railway;
- electricity;
- gas;
- government and government services (including local authorities);
- medical;
- water; and
- logistics.

In addition to the above, the Basic Policy for Critical Information Infrastructure Protection (3rd Edition), published by the Information Security Policy Council on 9 May 2014, has further added chemical industries, credit card services, and petroleum industries as critical information infrastructure sectors. Moreover, new network system services such as smart city and smart town, intelligent transportation system and other transportation control systems, etc, as well as defence industries and energy-related industries, which are included in the scope of critical infrastructure in the United States, will also continue to be considered, in line with environmental changes and based on coordination with related parties.

It is pertinent to mention that the Security Special Advisor to the Cabinet Secretariat has referred to IT systems such as websites, control systems of plants, and critical social infrastructures such as power plants, financial institutions, and broadcasting companies as possible cyberattack targets. The Advisor also mentioned that the promotion of the development and the strengthening of the international competitiveness of cybersecurity industries and the cultivation of human resources in the cybersecurity sector are the key points to be taken from the Basic Cybersecurity Act. Some universities and IT companies have already started joint activities towards cultivation of cybersecurity human resources.

3 Has your jurisdiction adopted any international standards related to cybersecurity?

The Japan Institute for Promotion of Digital Economy and Community (JIPDEC) operates an assessment system (ISMS conformity assessment system) for certifying whether or not the information security management system (ISMS) of a company is consistent with international standards. Under this assessment system, examinations are made as to whether an ISMS implemented by a company is in conformity with JIS Q 27001 (ISO/IEC 27001).

4 What are the obligations of responsible personnel and directors to keep informed about the adequacy of the organisation's protection of networks and data, and how may they be held responsible for inadequate cybersecurity?

Under the Personal Information Protection Act, a personal information handling business operator is required to take, in relation to information security, necessary and suitable measures for the prevention of any leakage, loss or damage of any personal data handled by it and for the security management of other personal data (article 20 of the Personal Information Protection Act). In addition, to ensure security management of personal data, the aforementioned business operator is required to perform the necessary and suitable supervision over its employees or contractors who handle personal data (articles 21 and 22 of the Personal Information Protection Act). As of 31 January 2014, 40 guidelines for 27 sectors have been developed by the respective government agencies, and the specific measures to be taken by the personal information handling business operator are prescribed in such guidelines.

If any personal information handling business operator violates its obligation to take security management measures, the competent authority may, where necessary, recommend or order that such personal information handling business operator cease the violation and take necessary measures for correcting the violation (article 34 of the Personal Information Protection Act). A business operator that violates any such order issued by the competent authority shall be sentenced to imprisonment with labour for not more than six months or be subject to a fine of not more than ¥300,000 (article 56 of the Personal Information Protection Act).

In the case of a large company, defined in article 2, item 6 of the Companies Act, the company must, in order to develop a system to ensure good governance of the company, decide on matters concerning internal regulations and other systems. Internal regulations concerning such risk management are general in nature, and they are typically not intended for ensuring cybersecurity. Provisions for ensuring cybersecurity, however, may be required to be made as part of the internal policies depending on the type or the volume of information held by the applicable large company or its business type.

Directors of a company limited by shares, if not a large company as defined in article 2, item 6 of the Companies Act, have a duty of due care of a prudent manager (article 330 of the Companies Act; article 644 of the Civil Code) to the company, and there is a possibility that any failure to develop a system for risk management constitutes a violation of the duty of care of a prudent manager. If a director is recognised to have violated the duty of due care of a prudent manager, the director shall be liable for providing compensation for damage caused thereby (article 423, paragraph 1 of the Companies Act).

5 How does your jurisdiction define cybersecurity and cybercrime?

In Japan, the term 'cybersecurity' has been legally defined for the first time in article 2 of the Basic Cybersecurity Act. The definition of cybersecurity is as follows:

> *The conditions where the measures necessary for the prevention of leakage, loss or damage, and for other security management of information which is recorded, sent, transmitted or received using an electronic method, a magnetic method, or any other method not recognisable to human senses, as well as measures necessary for securing the safety and reliability of information systems and information communication networks have been taken, and where such conditions are being properly maintained and managed.*

There is no clear comprehensive definition of the term 'cybercrime'; only the types of acts to be punished as a crime are prescribed in each of the criminal penalty provisions.

6 What are the minimum protective measures that organisations must implement to protect data and information technology systems from cyberthreats?

In terms of the Personal Information Protection Act, concrete security management measures to be taken by personal information handling business operators are prescribed in the guidelines developed by the respective government agencies, as provided in question 4.

For example, according to the guidelines targeting the financial sector, as prescribed by the Financial Services Agency, each personal information handling business operator (ie, financial institution) must take necessary and suitable measures as to the development of implementation structures for security management measures, for the prevention of leakage, loss, or damage, and for other management of security of the personal data that it handles. Further, it is prescribed in such guidelines that said measures must include 'systematic management measures', 'human security management measures', and 'technical management measures', which are laid out according to the respective levels of acquisition, usage, and retention of personal data.

7 Does your jurisdiction have any laws or regulations that specifically address cyberthreats to intellectual property?

Article 15 of the Basic Cybersecurity Act provides the obligation of the state to promote awareness of the importance of cybersecurity and to provide necessary information, advice and other necessary measures to private business operators and educational and research institutions to protect the intellectual property information held by them, in view of the importance of such intellectual property related information for the reinforcement of Japan's international competitiveness.

8 Does your jurisdiction have any laws or regulations that specifically address cyberthreats to critical infrastructure or specific sectors?

In order to provide stable and proper services, critical infrastructure operators are obligated to have a deeper understanding and should know the significance of cybersecurity. They are further required to make voluntary and active efforts to ensure cybersecurity and to cooperate in putting in place cybersecurity measures prescribed by the state or local authorities (article 6 of the Basic Cybersecurity Act). In addition, the Basic Cybersecurity Act prescribes that the government must develop basic schemes concerning cybersecurity ('cybersecurity strategies') for the furtherance of cybersecurity measures in an effective manner. It further provides that cybersecurity strategies must contain matters relating to strengthening cybersecurity in critical infrastructure operators (article 12, paragraph 2, item 3 of the Act). It is expected that, in furtherance of the enactment of the Basic Cybersecurity Act, the government will separately enact or develop specific laws, regulations, or guidelines, etc concerning matters to be complied with by critical infrastructure operators for ensuring cybersecurity.

9 Does your jurisdiction have any cybersecurity laws or regulations that specifically restrict sharing of cyberthreat information?

In Japan, it is construed that the spirit of article 13 of the Japanese Constitution guarantees privacy in general. The Personal Information Protection Act also deals with some aspects of privacy; however, there are no privacy-specific cybersecurity laws or regulations.

In terms of private communications, article 21, paragraph 2 of the Japanese Constitution guarantees the secrecy of communications, stating that: 'No censorship shall be maintained, nor shall the secrecy of any means of communication be violated.' It is prescribed in the Telecommunications Business Act that secrecy of communications handled by telecommunications business operators shall not be violated (not only by telecommunications business operators but also by any other person). The Radio Act also protects the secrecy of encrypted private communications.

As an exception to the above, the Act on Wiretapping for Criminal Investigation permits, as a special investigation method for serious crimes, the wiretapping of telecommunications for criminal investigations, based on strict requirements and subject to a warrant issued by a judge, with an observer being present throughout the process, limited to such cases where it would be difficult to reveal the truth through normal investigative means.

10 What are the principal cyberactivities that are criminalised by the law of your jurisdiction?

See question 24.

11 How has your jurisdiction addressed information security challenges associated with cloud computing?

Globalisation of corporate activities has facilitated cloud services and other transborder distribution of information. The Personal Information Protection Act is expected to be amended to create a better structure, keeping in mind the systems being used overseas. Amendments are required to update the Act to align it with the prevailing circumstances in the international society, and to bring it up to the required international standards, so that transborder distribution of information can be performed smoothly. Amendments are also required to prescribe protective measures to be taken when transferring information to other countries in a manner allowing application of Japanese laws to foreign business operators. The bill to amend the Personal Information Protection Act is planned to be laid before the Japanese parliament as soon as possible in 2015.

12 How do your jurisdiction's cybersecurity laws affect foreign organisations doing business in your jurisdiction? Are the regulatory obligations the same for foreign organisations?

Obligations under Japanese laws and regulations applicable to foreign corporations engaging in business in Japan are the same as those applicable to domestic corporations in Japan.

Best practice

13 Do the authorities recommend additional cybersecurity protections beyond what is mandated by law?

As stated in question 2, based on the recent enactment of the Basic Cybersecurity Act, the obligations for critical infrastructure operators, cyber-related business operators, university and other educational and research institutions shall be prescribed in a more concrete manner by the promulgation of specific laws and regulations that will be developed in the future. This may also include guidelines for strengthening cybersecurity. The guidelines mentioned in question 4, which have been provided from the perspective of information security, would also recommend additional protections.

14 How does the government incentivise organisations to improve their cybersecurity?

To ensure that critical infrastructure operators adhere to measures to strengthen cybersecurity, the Basic Cybersecurity Act requires the state to take necessary measures such as developing basic standards to be followed, providing drills, training and promoting information sharing and other voluntary efforts (article 14). In addition, the state is required to promote awareness regarding the significance of cybersecurity, hold consultations concerning cybersecurity, provide necessary information and advice and take other necessary measures (article 15). See also question 18.

15 Identify and outline the main industry standards and codes of practice promoting cybersecurity. Where can these be accessed?

With regard to information security, international standards ISO/IEC 27001, ISO/IEC 27002 and ISO/IEC 27017 are principally used in the development of relevant guidelines.

To use the ISO standards for the applicable certification system in Japan, however, the contents of such ISO standards must be established anew as Japanese Industrial Standards (JISs). JIS refers to national standards that are established in accordance with the Industrial Standardisation Act. These are specially enacted for the purpose of furthering industrial standardisation in Japan.

For example, as of December 2013, JIS Q 27000:2014, JIS Q 27001:2014, JIS Q 27002:2014, and JIS Q 27006:2012 have been established as national standards based on ISO/IEC27000 (issued in 2012), ISO/IEC27001 (issued in 2013), ISO/IEC27002 (issued in 2013) and ISO/IEC27006 (issued in 2011), respectively.

16 Are there generally recommended best practices and procedures for responding to breaches?

In the event of an accidental information leak at a company, although the measures to be taken by such company may vary depending on each case, generally speaking, examples of possible measures include the following:

- immediately verify related facts concerned, including causes of the accident and the information that has been leaked, and announce accurate facts at an early stage and express sincere apologies;
- continuously announce facts that may be revealed through subsequent investigations;
- perform investigations not only by a team of internal members, but also, where necessary or appropriate, organise a third-party committee consisting of legal specialists including attorneys and technical specialists, etc who are in neutral positions and cause investigations to be performed by such committee, and also report the results of the investigations performed; and
- develop and adopt measures to prevent recurrence based on the accidental information leak concerned.

17 Describe practices and procedures for voluntary sharing of information about cyberthreats in your jurisdiction. Are there any legal or policy incentives?

With regard to voluntary sharing of information relating to cyberthreats, there is no legal or political incentive in particular. From the perspective of information security, however, in the event of an accidental leak of information at a company, it would be practically advantageous for such company to make an accurate announcement at an early stage and to humbly take necessary measures in order to reduce the deterioration of goodwill among its customers.

18 How do the government and private sector cooperate to develop cybersecurity standards and procedures?

The Basic Cybersecurity Act provides the basic philosophy for cybersecurity and basic measures that are required to be taken 'for facing threats to cybersecurity, through coordination of various entities such as the state, local authorities, critical infrastructure operators, etc' (article 3). In order to realise such coordination, the Basic Cybersecurity Act requires the government or the state to take the following measures, in addition to the measures mentioned in question 14:

- necessary legal, financial or tax measures and other measures to be taken by the government to adhere to the policies concerning cybersecurity under the Basic Cybersecurity Act (article 10); and
- necessary measures to be taken by the state in order to reinforce coordination among relevant governmental agencies and ministries, and to enable various entities such as the state, local authorities, critical infrastructure operators, etc to mutually coordinate and work on cybersecurity-related measures (article 16).

19 Is insurance for cybersecurity breaches available in the jurisdiction and is such insurance common?

Insurance products covering 'cyber risks', such as standard attacks from outside parties and unauthorised access committed internally, providing coverage for damage arising from personal information leakage or system failure or such similar issues, are generally available. However, most of these insurance products have limited the types of incidents for which insurance benefits can be claimed for, and have also limited the place of insured incidents to Japan.

In December 2012, a Japanese corporation belonging to an insurance company group based in the United States started selling insurance products that provide broader coverage for damage arising from cyberattacks, including accidents occurring outside Japan.

Enforcement

20 Which regulatory authorities are primarily responsible for enforcing cybersecurity rules?

Government agencies that are the competent authorities concerning cybersecurity are the nodal authorities for ensuring implementation of the said laws, such as by providing their interpretations as relevant administrative organs and developing guidelines (provided, however, that the interpretation of laws by such administrative organs shall not be binding upon judicial organs).

Update and trends

Most of the critical infrastructure business operators are private entities, and, accordingly, there is an issue in relation to the possibility of excessively strict obligations being imposed on such entities resulting in pushback from such entities due to the huge expenses and manpower required from them in ensuring cybersecurity. In this regard, as mentioned in question 22, it can be said that such issue has been resolved by the Basic Cybersecurity Act being preconditioned on the furtherance of the voluntary efforts of private business operators, while limiting their obligations merely to making an effort to improve security of their systems. In addition, pursuant to the Basic Cybersecurity Act, the position of the cybersecurity strategy headquarters (the Chief Cabinet Secretary acting as the head of the headquarters) as an organisation demonstrating a control tower function extending across ministries and agencies has been made legally clear, allowing for the cybersecurity strategy headquarters to fulfil their roles in a more effective manner (as outlined in chapter 4 of the Basic Cybersecurity Act). Much attention is thus paid to the effective measures to be taken hereafter by the state in relation to cybersecurity under the leadership of the cybersecurity strategy headquarters.

The specific measures that are currently being considered concerning cybersecurity include the following.

The Financial Services Agency (FSA) is currently considering, and intends to reach a conclusion concerning, issues such as the possibilities of cyberattack-related incidents taking place at listed companies and indicting such possibilities to investors as business risks, etc, referring to the practices of the US Securities and Exchange Commission. With regard to the said issues, the FSA is also considering, and intends to reach a conclusion concerning, possible incentives for the furtherance of disclosure of such incidents.

The Ministry of Economy, Trade and Industry (METI) is now working on establishing Cybersecurity Management Guidelines that will describe desirable cybersecurity measures, set forth an organisational framework, including the appointment of a Chief Information Security Officer, and detail technical measures and information disclosure methods, etc.

Further, METI is considering establishing a third-party certification system under which a third party will assess whether or not companies are in compliance with the Cybersecurity Management Guidelines and are ensuring cybersecurity. In addition, METI is also considering legislation regarding the basic principles of the content, etc, of the Cybersecurity Management Guidelines in order to enhance the effectiveness thereof.

Further, in line with circumstances such as the need to make preparations for the Tokyo Olympic and Paralympic Games scheduled for 2020, as well as increased threats to cyberspace, related laws and regulations are likely to be developed and it will be necessary to pay careful attention to such developments.

For example, the National Police Agency, the Ministry of Internal Affairs and Communications, and the Ministry of Economy, Trade and Industry are the competent authorities in the case of the Unauthorised Computer Access Prohibition Act, and the Ministry of Justice has competency over laws pertaining to cybercrimes, including the Penal Code, and, as such, are in charge of the implementation of such laws. While the Consumers Affairs Agency has competency over the Personal Information Protection Act, as expressly prescribed in said Act, in the event of a personal information handling business operator being in violation of the obligatory provisions of the Personal Information Protection Act, and improperly handling personal information, the competent authority having jurisdiction over each business field may, where necessary, take measures such as requiring reports from (article 32 of the Personal Information Protection Act), providing advice to (article 33 of the Act) or recommendations or orders to (article 34 of the Act) such personal information handling business operator. In addition, the personal information handling business operator concerned shall be punished (chapter 6 of the Act) if it fails to comply with any order of the competent authority. Under the Amended Personal Information Protection Act, the power to collect reports and to provide advice, recommendations, directions, etc, which has previously been held by the competent ministers, will be delegated to the Personal Information Protection Commission.

21 Describe the authorities' powers to monitor compliance, conduct investigations and prosecute infringements.

With regard to cybersecurity, there are, to date, no laws or regulations directly and expressly prescribing the power of any administrative organ to monitor or investigate private business operators for their compliance with regard to the implementation of measures to strengthen cybersecurity. The obligation imposed on those other than the state or the local authorities under the Basic Cybersecurity Act are obligations to make efforts, and the Basic Cybersecurity Act itself will not be grounds for the authorities' power over private sectors. Therefore, no administrative organ has the power to prosecute any private business operator in the event of a violation of such obligations. See also question 18.

22 What are the most common enforcement issues and how have regulators and the private sector addressed them?

Administrative organs do not have the power to impose, by way of penalties, or by any other means, any mandatory obligations on private business operators to ensure cybersecurity. The Basic Cybersecurity Act is preconditioned on the fact that the obligations of parties, other than the state and local authorities, are limited to carrying out best efforts and the voluntary efforts of private business operators will be furthered by the state by taking necessary measures. This being the case, there is a huge issue in terms of whether or not voluntary efforts of private business operators can be effectively furthered based on measures taken by the state. Since there is no physical border and no safe space in the cyberworld, international cooperation towards enforcement is an important issue.

23 What penalties may be imposed for failure to comply with regulations aimed at preventing cybersecurity breaches?

To date, there is no penalty under law imposed on those parties who, because of not implementing sufficient measures for cybersecurity, have been victims of cyberattacks. It is, however, set forth in the Unauthorised Computer Access Prohibition Act that, an administrator of a computer connected to telecommunication lines, who has added an access control feature to such computer by way of an ID or password, has the obligation to always verify the effectiveness of such ID or password and endeavour to promptly take appropriate measures to protect the computer concerned from acts of unauthorised computer access, such as enhancement of the function of the access control feature concerned, whenever deemed necessary (article 8 of the Unauthorised Computer Access Prohibition Act). See also question 20 with regard to information security.

24 What penalties may be imposed for failure to comply with the rules on reporting threats and breaches?

With regard to cybersecurity, there is, to date, no law or regulation directly and expressly obliging a private business operator to report any cyberattack sustained by it, and no penalty is imposed on it in the event of a failure to make such report. On the other hand, in terms of information security, some of the guidelines prepared in accordance with the Personal Information Protection Act set forth an obligation to report any information leakage to the competent authority. For example, the Guidelines for Personal Information Protection in the Financial Field state: 'An entity handling personal information must immediately report to the supervisory authorities when an incident regarding leakage of personal information occurs' (article 22, paragraph 1). See also question 20.

25 How can parties seek private redress for unauthorised cyberactivity or failure to adequately protect systems and data?

If cybersecurity is regarded as a contractual obligation, compensation may, as a general rule, be claimed against a party who has such obligation, within the scope of a reasonable cause–effect relationship. It is, however, possible to restrict the scope of the damage compensation obligation, based on the mutual agreement of both parties to a contract, as long as such restrictions do not conflict with any mandatory laws and regulations. If such restriction is set forth in a contract, this merely means that compensation for damage may be made within such scope.

In the internet business, however, contracts could be entered into with consumers (ie, individuals, excluding those who become a party to

a contract in the course of, or for the interest of any business (article 2 of the Consumer Contract Act)). In such case, it should be fully noted that, according to the Consumer Contract Act, any clause that totally exempts a business operator from its liability to compensate a consumer for damage arising from default by the business operator is void (article 8 of the Act), and that such provision of the Act is a mandatory statute (ie, any clause of a contract in conflict therewith will be void).

Threat detection and reporting

26 What policies or procedures must organisations have in place to protect data or information technology systems from cyberthreats?

See question 6.

27 Describe any rules requiring organisations to keep records of cyberthreats or attacks.

To date, there are no rules directly and expressly prescribing such obligations, under any laws or regulations.

28 Describe any rules requiring organisations to report cybersecurity breaches to regulatory authorities.

See question 22.

29 What is the timeline for reporting to the authorities?

To date, there is no law or regulation directly and expressly prescribing the obligation of a private business operator to make regular reports concerning cybersecurity. Reporting obligations in the event of a leakage of information are discussed in question 24.

30 Describe any rules requiring organisations to report threats or breaches to others in the industry, to customers or to the general public.

In terms of information security, some of the guidelines established in accordance with the Personal Information Protection Act set forth matters relating to public announcements or notices to be provided in the event of any leakage of information. For example, the following is provided in the Guidelines for Personal Information Protection in the Financial Field: 'An entity handling personal information must promptly publicise the facts regarding the leakage accident and measures for preventing recurrence of the accident from a viewpoint of preventing secondary damage and avoiding the recurrence of similar accidents, in the event of an accidental leak of personal information' (article 22, paragraph 2); and 'An entity handling personal information in the financial field must notify the facts of the leakage accident promptly to the person whose personal information has been leaked, in the event of an accidental leak of personal information' (article 22, paragraph 3).

Masaya Hirano **mhirano@tmi.gr.jp**
Kazuyasu Shiraishi **kshiraishi@tmi.gr.jp**

23rd Floor, Roppongi Hills Mori Tower
6-10-1 Roppongi, Minato-ku
Tokyo 106-6123
Japan

Tel: +81 3 6438 5511
Fax: +81 3 6438 5522
www.tmi.gr.jp

Korea

Jin Hwan Kim, Brian Tae-Hyun Chung, Jennifer S Keh and Sung Min Kim
Kim & Chang

Legal framework

1 Summarise the main statutes and regulations that promote cybersecurity. Does your jurisdiction have dedicated cybersecurity laws?

In Korea, cybersecurity is mainly an issue in the context of privacy and data protection. As such, the main statutes that promote cybersecurity are the Personal Information Protection Act (PIPA) and the Act on the Promotion of IT Network Use and Information Protection (the Network Act), which are the representative laws relating to privacy and data protection.

More specifically, the PIPA and the Network Act prescribe:

- the technical and managerial protective measures that an entity must take to securely store personal information;
- measures that an entity must take in response to a data leakage incident;
- an entity's obligations regarding the protection of personal information, including the requirement to create and publish a privacy policy and the designation of a chief privacy officer;
- the requirements that an entity must meet in order to collect, use, transfer, outsource or otherwise process personal information; and
- the rights afforded to data subjects.

The PIPA applies to 'personal information processing organisations', which are defined as all persons, organisations, corporations and governmental agencies that process personal information for business purposes. The Network Act prescribes measures for protecting the personal information of users that is processed by 'online service providers,' which are defined as 'telecommunications service providers as prescribed in article 2, item 8 of the Telecommunications Business Act and other persons who provide information or act as an intermediary for the provision of information for the purpose of earning profit, by utilising the services rendered by telecommunications service providers.' Under this definition, online service providers include not only telecommunications service providers, but commercial website operators as well.

Korea does not have any dedicated laws devoted solely to cybersecurity.

2 Which sectors of the economy are most affected by cybersecurity laws and regulations in your jurisdiction?

To date, companies that operate their businesses online regardless of sector – such as portal sites, operators of online shopping sites and telecommunications companies – have made the most progress towards promoting cybersecurity. As these companies are constantly faced with the threat of cyberattacks due to the very nature of their business, they are strongly affected by laws addressing cybersecurity, which are intended to protect the data in their possession (such as customers' personal information) from cyberattacks.

In terms of specific sectors, companies in the financial sector are strongly affected, as their possession of highly valuable data has made them a frequent target of cyberattacks in Korea. In fact, companies in the financial sector are regulated more strictly in terms of cybersecurity compared with those in other sectors, as they are subject to the cybersecurity-related provisions of the Use and Protection of the Credit Information Act (the Credit Information Act) and the Electronic Financial Transactions Act, in addition to the PIPA and the Network Act.

3 Has your jurisdiction adopted any international standards related to cybersecurity?

Korea has not adopted any international standards relating to cybersecurity, but the following certifications issued by regulatory agencies consist of cybersecurity standards that are very similar to international standards, such as the ISO 27001:

- the Ministry of Science, ICT and Future Planning (MSIP) issues the Information Security Management System (ISMS) certification for evaluating whether a company has established or is operating a comprehensive management system that includes managerial, technical and physical protective measures to secure the safety and reliability of its information and communications network;
- the Korea Communications Commission (KCC) issues the Personal Information Management System (PIMS) certification for evaluating whether an entity has established or is operating a comprehensive management system that includes managerial, technical and physical protective measures for systematically and continuously engaging in actions to protect personal information in its information and communications network; and
- starting from 25 July 2016, the Ministry of the Interior (MOI) is expected to issue a certification for evaluating whether the measures taken by personal information processing organisations to process and protect personal information are in compliance with the PIPA.

4 What are the obligations of responsible personnel and directors to keep informed about the adequacy of the organisation's protection of networks and data, and how may they be held responsible for inadequate cybersecurity?

Korean laws do not expressly specify the obligations of responsible personnel and directors to keep informed of the organisation's protection of networks and data. However, under the PIPA and the Network Act, which prescribe specific security measures that must be taken by entities for the protection of personal information (see question 6), if failure to take the prescribed security measures leads to the loss, theft, leakage, alteration or damage of personal information, the responsible person, such as a company's chief privacy officer, can face criminal liability (see question 10). Additionally, if a financial institution fails to take adequate security measures pursuant to relevant laws, the Financial Supervisory Service (FSS), which regulates financial institutions in Korea, can impose administrative sanctions against the responsible personnel.

5 How does your jurisdiction define cybersecurity and cybercrime?

The following definitions apply under the National Cybersecurity Maintenance Regulation, which is an administrative regulation (that is less enforceable than a regulation and its corresponding presidential decree) that was established in connection with the protection of the national information network system:

- 'cybersecurity' is defined as 'protecting national information networks from cyberattacks and thereby maintaining the safety (ie, the security, integrity, availability, etc) of the national information and communications network and data;' and

- 'cyberattack' is defined as all forms of attack based on electronic means, including hacking, computer viruses, logic bombs, e-mail bombs, denial of service, etc, to unlawfully infringe, disturb, paralyse or destroy a national information and communications network, or steal or harm data.

However, as these definitions apply in the context of protecting national information and communications networks, they may not be as widely accepted by commercial entities.

There are no other relevant laws or case law definitions.

6 What are the minimum protective measures that organisations must implement to protect data and information technology systems from cyberthreats?

The PIPA and the Network Act include detailed technical security requirements and administrative requirements, which can be summarised as follows:

- the establishment and implementation of an internal management plan for the secure processing of personal information;
- the restriction of access rights to personal information;
- the installation and operation of an access restriction system (such as intrusion prevention systems and intrusion detection systems) for preventing illegal access to and leakage of personal information;
- the application of encryption technology to enable secure storage and transfer of personal information;
- the storage of access logs regarding access to the personal information processing system;
- the installation and updating of security programs;
- the establishment and implementation of password creation rules; and
- the taking of appropriate physical measures, such as the establishment of secure storage facilities for personal information and use of locking devices.

The Credit Information Act requires financial institutions to establish technical, physical and managerial security measures to defend against risks such as a third party's unlawful access to a credit information computer system, as well as the alteration, loss and destruction of inserted data.

Further, in order to ensure the security of electronic financial transactions and to protect electronic financial infrastructure and users, the Electronic Financial Transactions Act and its sub-regulations prescribe very specific standards for financial institutions on issues such as:

- labour force, organisation and budget;
- facilities such as buildings, equipment, data processing room, etc;
- information technology such as devices, data processing materials, information processing systems, information and communications networks, etc; and
- internal control systems.

7 Does your jurisdiction have any laws or regulations that specifically address cyberthreats to intellectual property?

No, Korea does not have laws or regulations that specifically address cyberthreats to intellectual property.

8 Does your jurisdiction have any laws or regulations that specifically address cyberthreats to critical infrastructure or specific sectors?

The Act on the Protection of Information and Communications Infrastructure (PICIA) specifically addresses cyberthreats to critical infrastructure and defines 'electronic intrusions' as acts of attacking information and communications infrastructures by hacking, computer viruses, logic or e-mail bombs, denial of service, or high power electromagnetic waves, etc. To protect critical information and communications infrastructures from electronic intrusion, the PICIA requires the analysis and evaluation of such infrastructures' vulnerabilities on a regular basis, and the establishment of security measures that are based on the said analysis and evaluation. Additionally, as explained in question 6, the Electronic Financial Transactions Act regulates the protection of electronic financial infrastructure in the financial sector.

9 Does your jurisdiction have any cybersecurity laws or regulations that specifically restrict sharing of cyberthreat information?

Korea does not have laws or regulations that specifically restrict sharing of cyberthreat information. However, the Communications Secrecy Act protects the constitutional right to keep private communications from infringement and it prohibits the censoring of a letter or document without a warrant issued by a court or a legal basis, the real-time wiretapping of telecommunications, as well as the recording of or listening to private communications. The Communications Secrecy Act also prescribes the requirements that must be met in order to censor letters or wiretap telecommunications on an exceptional basis.

10 What are the principal cyberactivities that are criminalised by the law of your jurisdiction?

The principal cyberactivities that are criminalised under applicable Korean laws can be summarised as follows.

Under the PIPA

Changing or deleting personal information being processed by public agencies and causing a severe hindrance, such as the suspension or paralysis of work performance by the public agencies in an attempt to disturb the processing of public information by public agencies, can result in imprisonment of up to 10 years or a fine of up to 100 million won.

Failure to take the requisite security measures leading to the loss, theft, leakage, falsification or damage of personal information can result in imprisonment of up to two years or a fine of up to 20 million won.

Under the Network Act

Providing or circulating a program with content that mutilates, destroys, alters or forges an information and communications system, data, program, etc or that interferes with the operation of such system, data, program, etc (ie, malware), through an information and communications network without justifiable grounds can result in imprisonment of up to five years or a fine of up to 50 million won.

Sending a large number of signals or data for the purpose of disrupting the safe operation of telecommunications systems or causing harm to the telecommunications system through methods such as forcing the processing of improper commands can result in imprisonment of up to five years or a fine of up to 50 million won.

Intruding on an information and communications network without proper access rights or by surpassing the scope of the permitted access rights can result in imprisonment of up to three years or a fine of up to 30 million won.

The failure to take the requisite security measures, which leads to the loss, theft, leakage, falsification or damage of personal information, can result in imprisonment of up to two years or a fine of up to 20 million won.

Under the Credit Information Act

Altering or deleting data from a credit information system without access rights or taking other measures to make such data unusable, or searching, copying or using other measures to use credit information without authorisation can result in imprisonment of up to five years or a fine of up to 50 million won.

Under the Electronic Financial Transactions Act

Intruding on electronic financial infrastructures without proper access rights or by surpassing the scope of the permitted access rights or altering, destroying, concealing or leaking data that is saved in such electronic financial infrastructures can result in imprisonment of up to 10 years or a fine of up to 100 million won.

Destroying data, or deploying a computer virus, logic bomb or program such as an e-mail bomb for the purpose of disrupting the operations of electronic financial infrastructures can result in imprisonment of up to 10 years or a fine of up to 100 million won.

Taking measures to cause errors or to disable the electronic financial infrastructure such as the sending of a one-time large-scale signal, high-powered electromagnetic wave or data, or requiring improper commands for the purpose of disrupting the safe operation of the electronic financial infrastructure can result in imprisonment of up to 10 years or a fine of up to 100 million won.

Under the PICIA
Disturbing, paralysing or destroying critical information and communications infrastructure can result in imprisonment with labour for not more than 10 years or a fine not exceeding 100 million won.

Under the Communications Secrecy Act
The censoring of a letter or document without a warrant issued by a court or a legal basis or the real-time wiretapping of telecommunications, as well as the recording of or listening to private communications, among others, can result in imprisonment of between one and 10 years and loss of qualification for up to five years.

11 How has your jurisdiction addressed information security challenges associated with cloud computing?

The Cloud Computing Development and User Protection Act became effective on 28 September 2015. This Act includes regulations to promote the development and use of cloud computing services and states that the MSIP can establish and issue a notification for standards on the quality and performance of cloud computing services and data protection (which includes managerial, physical and technical security measures), and require cloud computing service providers to meet those standards. Currently, preparations are underway for preparing detailed standards, and once the MSIP issues its notification on the standards, we can expect additional public discussion on practical matters concerning security challenges associated with cloud computing.

12 How do your jurisdiction's cybersecurity laws affect foreign organisations doing business in your jurisdiction? Are the regulatory obligations the same for foreign organisations?

Korea's cybersecurity laws do not specifically address the issue of whether they apply to foreign organisations. However, they do not differentiate between the obligations imposed on foreign and local organisations. In fact, in January 2014, the KCC fined a multinational corporation approximately 200 million won for collecting Korean users' personal information without properly obtaining their consent. This was the first time that the KCC imposed an administrative fine directly on a foreign organisation.

Best practice

13 Do the authorities recommend additional cybersecurity protections beyond what is mandated by law?

Yes. Regulatory authorities recommend additional cybersecurity protections beyond that which is mandated by law by issuing and promoting certifications. (For additional information, see question 3.)

14 How does the government incentivise organisations to improve their cybersecurity?

Entities that obtain certifications issued by regulatory authorities can receive additional credit when they participate in bids for public projects. Additionally, the fact that they are certified can act as a mitigating factor in the event that they are subsequently involved in an alleged violation of the law.

15 Identify and outline the main industry standards and codes of practice promoting cybersecurity. Where can these be accessed?

In Korea, as security measures on cybersecurity are already incorporated in various regulations, companies are not actively engaged in establishing industry standards and codes of practice. However, as explained in question 3, the MSIP and the KCC issue the ISMS and PIMS certifications, respectively, and related standards can be accessed at www.isms.kisa.or.kr, which is operated by the Korea Internet Security Agency (KISA), the enforcing arm of the KCC. (Please note that this website only provides information in Korean.)

16 Are there generally recommended best practices and procedures for responding to breaches?

In Korea, there are strict security requirements that companies must meet to ensure data protection, as well as various substantial liabilities, including criminal penalties, which can be imposed on companies and affiliated employees in connection with data breaches. To minimise the risk of such liabilities, it is advisable to receive legal guidance not only in connection with investigations conducted by regulatory authorities, but also regarding communications with affected data subjects and public relations.

17 Describe practices and procedures for voluntary sharing of information about cyberthreats in your jurisdiction. Are there any legal or policy incentives?

Upon becoming aware that cyberthreats such as intrusion incidents exist, regulatory authorities such as the MSIP, the FSC, and KISA share relevant information with the public so that companies can prevent or mitigate potential harm. There are no legal or policy incentives to encourage the voluntary sharing of information about cyberthreats among companies.

18 How do the government and private sector cooperate to develop cybersecurity standards and procedures?

Once a regulatory authority establishes policies or guidelines concerning data protection or cybersecurity, it obtains and incorporates comments provided by entities in the private sector.

19 Is insurance for cybersecurity breaches available in the jurisdiction and is such insurance common?

Insurance for liability resulting from cybersecurity breaches is available in Korea, but currently it is not common for businesses to have this type of insurance. However, the number of businesses purchasing this type of insurance is expected to rise.

Enforcement

20 Which regulatory authorities are primarily responsible for enforcing cybersecurity rules?

The regulatory authorities that are responsible for enforcing the cybersecurity-related provisions of various laws can be summarised as follows:

- for the PIPA: the MOI;
- for the Network Act: the KCC and the MSIP; and
- for the Credit Information Act, the Electronic Financial Transactions Act and other rules concerning the protection of information held by financial institutions: the FSS.

Additionally, the above laws provide criminal sanctions as penalties for violations and, to the extent that they apply, the corresponding criminal investigation and indictment proceedings will be handled by the police and the prosecutor's office.

21 Describe the authorities' powers to monitor compliance, conduct investigations and prosecute infringements.

In order to confirm a company's compliance with various laws, regulatory authorities can request the submission of documents or materials, as well as conduct on-site investigations.

For example, to check whether companies are in compliance with the PIPA, the MOI can make requests for information and conduct on-site inspections at the premises of companies.

The KCC and the MSIP, which are responsible for enforcing the Network Act, are both authorised to take measures similar to those that can be taken by the MOI. Further, under the Network Act, if there is an 'intrusion incident' (which is defined under article 2 as 'an incident that is caused by an attack on the information network or the related information system through hacking, computer virus, logic bomb, e-mail bomb, denial of service, high-powered electromagnetic wave, etc'), the MSIP can also request the submission of materials or conduct an on-site investigation in order to determine the cause of the incident.

Finally, the FSS, as the regulatory authority tasked with enforcing the Electronic Financial Transactions Act, has broad authority to request the submission of materials and conduct in-person interviews with responsible persons in order to oversee and investigate whether financial institutions are in compliance with their legal obligations.

22 What are the most common enforcement issues and how have regulators and the private sector addressed them?

If there is a security incident such as a leakage of personal information caused by hacking, which could result in corporate liability, regulators commence investigations to check the company's overall compliance with related regulations without limiting themselves to the particular security incident at issue. As a result, if a company's non-compliance is confirmed during the course of an on-site investigation, regulators typically impose penalties based on the particular violations at issue. (See question 23, for additional information on penalties that apply specifically for failure to comply with regulations aimed at preventing cybersecurity breaches.)

As a notable example, in March 2014, it was confirmed that a major telecommunications carrier was hacked, and the personal information of over 10 million customers was compromised as a result. In response, the KCC and the police commenced investigations on the carrier in addition to their investigations on the hacker. The carrier successfully defended the claims in the criminal investigation, but the KCC imposed an administrative fine. The carrier appealed the KCC's decision and the resulting litigation is currently ongoing.

23 What penalties may be imposed for failure to comply with regulations aimed at preventing cybersecurity breaches?

The penalties that can be imposed under the various applicable laws can be summarised as follows:

- failure to comply with PIPA and the Network Act's detailed technical and security measures may subject a company to administrative fines of up to 30 million won;
- failure to comply with the technical, physical and managerial security measures prescribed by the Credit Information Act can result in administrative fines of up to 50 million won; and
- failure to comply with the safety measures required under the Electronic Financial Transactions Act and its sub-regulations can result in administrative fines of up to 50 million won.

As a general matter, regulatory authorities are authorised to issue corrective orders to non-complying companies. Additionally, if failure to take the requisite security measures leads to the loss, theft, leakage, falsification or damage of personal information, criminal penalties can be imposed under the PIPA and the Network Act. (For additional information, see question 10.)

Finally, under the Network Act, the KCC can impose an administrative fine of up to 3 per cent of the relevant sales revenue for any loss, theft, leakage, falsification or damage of personal information of data subjects resulting from an online service provider's failure to take the required security measures.

24 What penalties may be imposed for failure to comply with the rules on reporting threats and breaches?

Under the Network Act, if there is an intrusion incident, the affected online service provider is obligated to report the incident to the MSIP or the KISA, and the failure to meet this reporting requirement can result in an administrative fine of up to 10 million won. The Network Act also requires online service providers to report any leakages of personal information to the KCC or KISA. This requirement is triggered regardless of the number of affected data subjects (unlike the PIPA's reporting requirement for personal leakage incidents), and the failure to meet this requirement can lead to administrative fines of up to 30 million won.

Under the Electronic Financial Transactions Act, if an electronic intrusion leads to an accident, such as the disruption or paralysis of the electronic financial infrastructure, a financial institution must notify the Financial Services Commission (FSC) without delay. The failure to meet this notification requirement can result in administrative fines of up to 10 million won.

Update and trends

There are no particular challenges to developing cybersecurity regulations in Korea and companies can help shape a favourable regulatory environment by meeting their obligations under relevant data protection laws. Due to the growing awareness of data protection issues and relevant laws such as the PIPA and the Network Act among individual data subjects as well as companies, cybersecurity laws and policies are expected to become more protective of personal information and privacy rights. Various amendments to data protection laws are currently being debated at the National Assembly, and their impact on Korean data protection laws remains to be seen.

Under the PIPA, upon becoming aware of the fact that personal information of over 10,000 individuals was leaked, a personal information processing organisation is obligated to file a personal information leakage report to the MOI or KISA. Failure to meet this requirement can result in an administrative fine of up to 30 million won.

25 How can parties seek private redress for unauthorised cyberactivity or failure to adequately protect systems and data?

Parties can seek private redress (from organisations and individuals) by commencing litigation for damages, alleging that the unauthorised cyberactivity or failure to adequately protect systems and data constitutes illegal conduct under applicable laws such as the Civil Code. Parties can also seek statutory damages of up to 3 million won under the Network Act if an online service provider's breach of the Network Act results in the loss, theft or leakage of the parties' personal information, and a statutory damages scheme will also be available under the PIPA from 25 July 2016. In addition, from 25 July 2016, courts can award treble damages if the personal information processing organisation's wilful misconduct or gross negligence causes the loss, theft, leakage, falsification or damage of personal information.

Threat detection and reporting

26 What policies or procedures must organisations have in place to protect data or information technology systems from cyberthreats?

See question 6.

27 Describe any rules requiring organisations to keep records of cyberthreats or attacks.

Under the Network Act, the MSIP can request a company to keep records relating to cyberthreats or attacks, such as access records for information and communications networks and other relevant materials, if it finds that such information and materials are necessary for analysing the underlying cause of the intrusion incident.

KIM & CHANG

Jin Hwan Kim **jhkim4@kimchang.com**
Brian Tae-Hyun Chung **thchung@kimchang.com**
Jennifer S Keh **jennifer.keh@kimchang.com**
Sung Min Kim **sungmin.kim1@kimchang.com**

Seyang Building
39 Sajik-ro 8-gil, Jongno-gu
Seoul 03170
Korea

Tel: +82 2 3703 1114
Fax: +82 2 737 9091 / 9092
www.kimchang.com

28 Describe any rules requiring organisations to report cybersecurity breaches to regulatory authorities.

See question 24.

29 What is the timeline for reporting to the authorities?

In cases where a report to the relevant authorities is required, the timeline for reporting is 'without delay' regardless of whether it is for an intrusion incident or a leakage of personal information.

30 Describe any rules requiring organisations to report threats or breaches to others in the industry, to customers or to the general public.

Under the PIPA, upon becoming aware of the fact that personal information was leaked, a personal information processing organisation must provide individual notice to data subjects regarding the following:

- the items of personal information that were subject to the leakage;
- the time and underlying context of the leakage;
- information on the measures that the data subject can take to lessen the damage that may arise in connection to the leakage;
- the measures that the personal information processing organisation is taking in response to the leakage and to lessen the damage; and
- the name and contact information of the relevant department that the data subject can contact if he or she is harmed by the leakage.

Individual notice must be provided via email, fax, telephone, text message or a similar method.

The Network Act imposes similar requirements to online service providers. Failure to meet the notification requirements under both the PIPA and the Network Act can result in an administrative fine of up to 30 million won.

Malta

Olga Finkel and Robert Zammit
WH Partners

Legal framework

1 Summarise the main statutes and regulations that promote cybersecurity. Does your jurisdiction have dedicated cybersecurity laws?

Malta has not enacted dedicated cybersecurity legislation; however, as a member of the European Union and the Council of Europe, it must fully conform to its obligations resulting therefrom. To this end, in 2001 a subtitle was added to the Criminal Code entitled 'Of Computer Misuse', which largely incorporates the provisions of the Council of Europe Cybercrime Convention, which itself was fully ratified by Malta in 2012.

Under the Criminal Code, article 337C criminalises unlawful access to, or use of, information. Among the offences criminalised under this article is the unlawful use of a computer or other device or equipment to access any data, software of supporting documentation held in that computer or on any other computer, or uses, copies or modifies any such data, software or supporting documentation. This article also criminalises unauthorised activities that hinder access to any data, and also covers the unlawful disclosure of data or passwords. The following article 337D then criminalises the misuse of hardware. One of the most striking features of the Computer Misuse subtitle in the Criminal Code is the evident technological neutrality, which will allow these criminal laws to cater for a host of unlawful activities, irrespective of the technological complexities at issue.

The Data Protection Act 2001, together with subsidiary legislation enacted under it, forms a legislative framework that implements EU directives, regulations and recommendations relating to privacy, including privacy in the electronic communications sector. This law imposes security obligations upon processors of personal data, whether it is collected, processed and stored via automated means or otherwise, and creates rights for the data subject with regard to personal and sensitive personal information held by data controllers.

The Electronic Communications Networks and Services (General) Regulations (SL 399.28) imposes requirements on providers of electronic communication services to ensure the security and integrity of networks from incidents, threats or vulnerabilities. An undertaking providing publicly available electronic communications services over public communications networks must take all necessary measures to ensure the fullest possible availability of such services in the event of a catastrophic network breakdown.

In certain sectors, such as financial services and remote gaming, information security requirements are imposed by way of sector-specific rules and supervision by licensing authorities.

2 Which sectors of the economy are most affected by cybersecurity laws and regulations in your jurisdiction?

In general, the size of Malta-based enterprises is small and the costs of proper data security measures can be quite high. Therefore, overall, it is regulated industries and e-government itself that led the way in the field of cybersecurity. The fields that have experienced both heightened growth via the web and mobile channels and are also involved in handling high volumes of sensitive data are the industries that have responded to cybersecurity challenges most. Among these are electronic (including mobile), banking, payments, telecommunications, e-government services, web-service providers and co-location centres, and remote gaming. Other sectors lag behind.

3 Has your jurisdiction adopted any international standards related to cybersecurity?

The chief international standard adopted in Malta is the ISO 27001, adopted by a number of organisations and governmental bodies in Malta to govern their information security management operations. Other organisations choose to implement the provisions of this standard without obtaining the corresponding certification. This standard is adopted, however, on a voluntary basis and, where an obligation to maintain certain levels of cybersecurity exist, adoption of this standard acts as a presumption that sufficient measures have been taken.

4 What are the obligations of responsible personnel and directors to keep informed about the adequacy of the organisation's protection of networks and data, and how may they be held responsible for inadequate cybersecurity?

Generally speaking, a company's affairs are managed by the board of directors who are responsible for the company's performance of its obligations.

From a data protection legislation perspective, the data controller is obliged under the Data Protection Act to implement appropriate technical and organisational measures to protect the personal data processed against accidental destruction or loss or unlawful forms or processing. The security measures to be implemented must give regard to the technical possibilities available, the cost of such measures, the special risks relating to the processing of the data, and the sensitivity of the data being processed. There are no explicit or specific legislative provisions further to the above.

Data controllers may be held responsible for inadequate cybersecurity by the Information and Data Protection Commissioner, who may order rectification of breach and may also institute civil legal proceedings where provisions of the Act have been or are about to be violated, and to refer any criminal offences encountered by reason of his functions to the competent public authority. Criminal penalties may be applicable to breaches of information security under this Act.

In regulated sectors, such as financial services and remote gaming, service providers undergo certification and supervisory checks, where they have to show and justify that the security measures taken are proportionate and adequate to the risks. In the event the supervisory body is not satisfied, the providers may either be refused a licence, or face fines or suspension of their licence, or both.

In addition, in the financial services sector, licence holders are being increasingly required to set up an internal audit function that is independent from the operational activities. The principal purpose of such audit would be to assess the appropriateness of the service provider's internal policies and procedures, including information security and risk management policies, and would review the compliance by the organisation with the same. Findings are reported to the board of directors of the organisation.

5 How does your jurisdiction define cybersecurity and cybercrime?

At present, specific definitions of cybersecurity and cybercrime do not exist in Malta's statutes or case law. One may, however, find guidance to these terms in the Criminal Code subtitle relating to Computer Misuse, which defines a 'computer' as an electronic device that performs logical arithmetic and memory functions by manipulating electronic or magnetic impulses, and includes all input, output, processing, storage, software and

communication facilities that are connected or related to a computer in a computer system or computer network. 'Computer data' here is defined as any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function. These definitions thus allow for broad scope to be afforded to the computer-related crimes of unauthorised access, use or modification of computing systems, software, hardware and data foreseen in this subtitle.

6 What are the minimum protective measures that organisations must implement to protect data and information technology systems from cyberthreats?

There are only generic requirements under applicable legislation relating to cybersecurity, stating that the security of systems must be adequate in relation to the sensitivity of information and repercussions that may arise as a result of information security breaches. There are no explicit or specific legislative requirements in addition to the above. However, those companies that are obliged to maintain adequate security in their business (such as financial services, telecoms, remote gaming) and normally have to undergo supervisory checks by their licensing authorities, normally adopt ISO 27001 standard. Moreover, financial service providers having to undergo PCI compliance generally follow the applicable rules as well with regard to storing of data and its encryption.

In the financial services sector, while applicable financial service legislation does not contain any mandatory requirements concerning certification of data centres or software applications to be used by financial businesses, during the application phase, the supervisory authority will consider the proposed IT structure on a case-by-case basis and will expect the applicant to identify reputable data centres and software providers that will enhance its ability to ensure continuous and regular provision of the licensed financial activities and adequate protection of customer data.

7 Does your jurisdiction have any laws or regulations that specifically address cyberthreats to intellectual property?

Malta does not at present have any laws or regulations that cater for cyberthreats to intellectual property. For the purposes of data security, unauthorised access to or misuse of data, data protected by intellectual property rights is treated in the same way as any other data.

8 Does your jurisdiction have any laws or regulations that specifically address cyberthreats to critical infrastructure or specific sectors?

The Criminal Code provisions in relation to computer misuse are made applicable to 'computer networks', 'software', 'hardware' and 'computer systems', which are defined widely and with enough technological neutrality to incorporate all conceivable cyberthreats to any technological infrastructure. These are the provisions that at present address cyberthreats to critical infrastructure. It must also be noted that in the Maltese government's Digital Malta strategy presented in March 2014 entitled the 'National Digital Strategy for 2014–2020', a National Cyber Security Strategy is planned for the coming years, which will include rules for the protection of critical infrastructure.

9 Does your jurisdiction have any cybersecurity laws or regulations that specifically restrict sharing of cyberthreat information?

In addition to the provisions of the Data Protection Act and subsidiary legislation, the Electronic Communications Networks and Services (General) Regulations (SL 399.28) address data protection issues arising from the use of electronic communications networks and services, whether these are public or non-public.

These regulations impose requirements on providers and communications and services to ensure the security and integrity of networks from incidents, threats or vulnerabilities, including personal data breaches. An undertaking providing publicly available electronic communications services over public communications networks must take all necessary measures to ensure the fullest possible availability of such services in the event of a catastrophic network breakdown.

Under Maltese law, private communications can only be intercepted by the Maltese Security Service upon obtaining a warrant signed by the Minister under the circumstances related to national security delineated in the Security Service Act.

10 What are the principal cyberactivities that are criminalised by the law of your jurisdiction?

The principal cyberactivities criminalised under article 337C of the Criminal Code are the unauthorised:

- use of a computer or other device to access, use, copy or modify data or other information held;
- output of data or other information from the computer where it is held in any manner whatsoever;
- copying of data or other information to a storage medium or other location other than that in which it is held;
- prevention or hindering of access to such data;
- hindering or impairing the functioning or operation of a computer system, software or the integrity or reliability of any data;
- possession of or use of data;
- installation, alternation, moving, damaging, deletion, deterioration, suppression, destruction, variation or addition of any data or other information;
- disclosure of a password or other form of access to an unauthorised person;
- interception by technical means of data transmissions; or
- production or any other form of procurement of a device, including a computer program, which is designed or adapted for the committing of the above-mentioned acts.

Breaches of the obligations and duties under the Data Protection Act and the Electronic Communications Act may also result in criminal sanctions.

11 How has your jurisdiction addressed information security challenges associated with cloud computing?

Maltese regulatory authorities have not as yet addressed the cybersecurity challenges emerging from the growing cloud computing sector through specifically targeted regulations.

Current policy frameworks seek to mitigate risks, while at the same time seizing the full benefits of cloud computing. This can be seen, for instance, in the licensing approach carried out at present by the Maltese Gaming Authority, Malta's public regulatory body responsible for all forms of gaming, where requests for use of the public or private cloud are dealt with on a case-by-case basis during the licensing process of a remote gaming operator. The same approach is to be seen with respect to financial services licence applications before the Malta Financial Services Authority (the single regulator of financial services in Malta).

12 How do your jurisdiction's cybersecurity laws affect foreign organisations doing business in your jurisdiction? Are the regulatory obligations the same for foreign organisations?

Malta's current cybersecurity laws largely transpose European directives and standards, and must comply with standards and rules contained in directly applicable European Union regulations. As a result of this, foreign jurisdictions would not be prejudiced by local rules when choosing to carry out their business in Malta.

Best practice

13 Do the authorities recommend additional cybersecurity protections beyond what is mandated by law?

The chief international standards relating to information security are ISO 27001 and 27002 security standards. Several organisations choose to implement the provisions of these standards in order to reduce risks to their computers and networks, without obtaining the corresponding certification.

14 How does the government incentivise organisations to improve their cybersecurity?

Capital investments made in relation to an organisation's information technology infrastructure may be eligible for tax credits on the expenditure incurred under the Micro Invest Scheme, promoted by the Maltese government agency responsible for providing fiscal and other incentives to business, the Malta Enterprise.

15 Identify and outline the main industry standards and codes of practice promoting cybersecurity. Where can these be accessed?

In the local telecommunications industry, one such code of conduct, signed by the major industry players, exists, promoting cybersecurity in accordance with the European Framework for Safer Mobile Use by Young Teenagers and Children to which they are signatories. This code of conduct relates to the content provided by the communications providers, and not to internet content in general. This code of conduct is publicly available and may be accessed on the telecommunications providers' websites.

16 Are there generally recommended best practices and procedures for responding to breaches?

In the remote gaming business, the best practices currently in place are the safe-keeping of all data related to the cyberthreat, the setting up of a dedicated team to identify the source of the threat and ensure proper steps are taken to avoid recurrence of such incident, and the education of the employees to ensure that all employees are aware of the threats and the importance of following the company's procedures and policies. Where necessary, third-party firms are engaged to perform penetration tests to ensure that the systems used are adequately secure.

17 Describe practices and procedures for voluntary sharing of information about cyberthreats in your jurisdiction. Are there any legal or policy incentives?

At present, there do not exist any legal or policy incentives targeting the voluntary sharing of information relating to cyberthreats as such.

18 How do the government and private sector cooperate to develop cybersecurity standards and procedures?

The process of enacting legislation and regulations applicable to the cybersecurity and ICT field is one that involves detailed discussions and consultation briefings involving key industry players, stakeholders in the field, and the general public to pool ideas with governmental bodies. This helps to ensure that regulations created for this field in which newer and more complex risks are constantly emerging are efficiently targeted in the creation of cybersecurity standards and procedures.

19 Is insurance for cybersecurity breaches available in the jurisdiction and is such insurance common?

Insurance coverage for cybersecurity threats is increasing in popularity in Malta at the same time as information technology companies continue to set up their businesses here. As cybersecurity breaches are becoming a major risk for modern data-centric organisations, it is beneficial to cover this risk in an appropriate insurance policy that can cover data loss incidents, business interruptions and network outages. However, while an insurance policy can cover the financial risks associated with security breaches, including the damages caused to third parties, no policy can ever bring back lost data or recall leaked sensitive information or erase potential reputational damage. Accordingly, insurance policies are not a substitute for, and should always work in conjunction with, data security policies and processes that minimise the risk in the first place.

Enforcement

20 Which regulatory authorities are primarily responsible for enforcing cybersecurity rules?

The Information and Data Protection Commissioner is the person authorised by the Data Protection Act to ensure and enforce compliance with the provisions of the Data Protection Act.

The Maltese Police Force set up a dedicated Cyber Crime Unit in 2003, whose main function is to provide technical assistance in the detection, investigation and prosecution of crime wherein the computer is the target or the means used. The Cyber Crime Unit is made up of police officers who are trained in the investigation of crimes that take place over the internet or through the use of a computer.

In addition, sectoral regulatory bodies may initiate and carry out enforcement through licensing and fine mechanisms.

21 Describe the authorities' powers to monitor compliance, conduct investigations and prosecute infringements.

Sectoral authorities, in general, have powers of requesting documentation, making site visits, conducting investigations and reporting to other competent bodies (such as the police) on their findings.

For example, in exercising his functions the Information and Data Protection Commissioner is empowered to enter and search any premises under the powers that are vested in executive police by any law. Similar powers are afforded to the Maltese Financial Services Authority. In particular, the Financial Services Authority requires applicants for a financial services licence to implement an IT and operational setup where the master data is located in Malta (or where this is not so, where replicated, back-up data is located in Malta). The Authority will require applicants to ensure that it will at all times have unrestricted control and direct and immediate access to the data in Malta so that the Authority's inspectors can at any time access such data to enable it to exercise its supervisory powers. Similarly the Maltese Gaming Authority requires applicants for remote gaming licences to have in place an information security policy whose aim is to safeguard data, applications, equipment and network, as well as a strict system access control policy to ensure that access is limited to the system as well as physical access being limited to on a need-to-know basis. Without the implementation of such policies, among other required policies, remote gaming applicants will not be granted a licence to operate in the remote gaming business from Malta. Audits are performed by appointed technical auditors to ensure that these policies are being followed.

The Maltese Police Cyber Crime Unit is charged with the investigation of criminal acts commonly associated with technology, as well as the investigation of more traditional offences such as fraud and threats perpetrated by cyber means. It is charged with the analysis and seizure of digital evidence collected in connection with investigations as well as in identifying persons committing crimes over the internet.

22 What are the most common enforcement issues and how have regulators and the private sector addressed them?

Criminal enforcement of breaches of cybersecurity against perpetrators is extremely low due to the fact that the crimes are often perpetrated from outside Malta and there is great difficulty in enforcement in such cases. The inability to prosecute is the most acute problem arising in enforcement of criminal cases relating to breaches of cybersecurity. Authorities will have to collaborate with foreign counterparts to be able to identify and arraign perpetrators. Companies located in Malta generally fully cooperate with police and provide information and access to their data and networks to assist in the investigation of crimes.

23 What penalties may be imposed for failure to comply with regulations aimed at preventing cybersecurity breaches?

The penalties applicable under the Data Protection Act may vary from fines ranging between €120 and €23,300 and imprisonment of not more than six months. The criminal penalties vary depending on the provisions of the Act being breached. On encountering a breach of the Act, which could lead to criminal proceedings, the Commissioner is to refer the situation to the competent authorities who in turn would need to take action in the criminal courts of Malta.

Other breaches of the Act may result in administrative fines, which can vary from one-time fines of up to €23,300 and daily fines of up to €2,500, depending on the provisions of the Act being breached.

In the remote gaming sector, should operators be found not in compliance with their information security policy and system access control policy the Gaming Authority would request the operators to take adequate actions to ensure compliance. Should this be not done to the satisfaction of the authority fines may be imposed.

In the financial sector, the Maltese Financial Services Authority reserves the right to impose certain sanctions where the entity no longer fulfils the conditions required for the granting of the licence generally. Such sanctions include the revocation or restriction of a licence and the imposition of administrative penalties where there is a breach of applicable financial services legislation.

24 What penalties may be imposed for failure to comply with the rules on reporting threats and breaches?

Article 3A of the Processing of Personal Data (Electronic Communications Sector) Regulations requires providers of publicly available electronic

communication services to notify a personal data breach to the Information and Data Protection Commissioner, and, where the personal data breach is likely to adversely affect the personal data of privacy of a subscriber or individual, such subscriber or individual, without undue delay. Contravention of or non-compliance with the provisions of these Regulations may lead to a penalty not exceeding €23,293.73 for each violation, and €2,329.37 for each day during which the violation persists. This fine is of an administrative nature, and shall be determined by the Information and Data Protection Commissioner.

Regulations 55 and 56 of the Electronic Communications Networks and Services (General) Regulations (Subsidiary Legislation 399.28) require undertakings providing network elements or service to inform the Maltese Communications Authority, inter alia, of any significant risk of a breach, or any actual, significant breach of the security or integrity of the services or network or failure or serious degradation of international connectivity. Any person suffering loss or damage because of any contravention of these Regulations shall be entitled to take action before the competent court or tribunal, seeking compensation from the person who caused the loss or damage.

Finally, data controllers operating in certain sectors, such as in the financial services sector, may be required by the relevant authority to disclose any personal data or security breach.

25 How can parties seek private redress for unauthorised cyberactivity or failure to adequately protect systems and data?

Private parties may seek private redress under the provisions of the Civil Code.

Threat detection and reporting

26 What policies or procedures must organisations have in place to protect data or information technology systems from cyberthreats?

The Data Protection Act provides that the carrying out of data processing by way of a processor is to be governed by a contract or other legally binding instrument, which must stipulate that the processor shall act only upon instructions from the data controller and shall implement all the necessary technical and organisational measures to ensure the protection of the data, by providing sufficient security.

The Electronic Communications Networks and Services (General) Regulations impose an obligation on undertakings providing connection to public communications networks or other publicly available electronic communications services to ensure the implementation of a security policy with respect to the processing of personal data. Appropriate security measures must be taken to prevent and minimise the impact of security incidents on users and interconnected networks. International gateway operators must additionally, at all times, adopt appropriate measures to safeguard the integrity and resiliency of the network elements utilised to provide international connectivity, and to secure the availability of capacity or have alternative measures in place to ensure an adequate level of uninterrupted international connectivity.

27 Describe any rules requiring organisations to keep records of cyberthreats or attacks.

Electronic communications providers are bound to retain categories of data pertaining to call and SMS logs, and internet data such as IP addresses, however no content records may be collected or stored.

Civil legal proceedings brought under the provisions of the Civil Code and the Code of Civil Procedure may be brought within a prescriptive period of five years. For this reason, it is advisable that records are kept for a period of five years from the date of the cyberthreat or attack in question.

The Prevention of Money Laundering and Funding of Terrorism Regulations (SL 373.01) may have cybersecurity implications. Under these Regulations, records of threats, identity information, and records of all business transactions must be kept for a minimum period of five years from the date on which the relevant transaction or financial business was completed.

Further, in the remote gaming sector the Gaming Authority requires operators to report situations of attacks on their system. These reports need to be prepared and submitted to the Authority within 24 hours of the incident and a copy of report is kept at the company's registered address.

28 Describe any rules requiring organisations to report cybersecurity breaches to regulatory authorities.

The European Commission Regulation 611/2013 provides for measures relating to the notification of personal data breaches under Directive 2002/58/EC (the ePrivacy Directive) application to electronic communications providers. This Regulation applies to providers of publicly available electronic communications services, who are obliged to notify the competent national authority of a personal data breach. Information that must be notified to the competent national authority in an initial report of a personal data breach comprises the date and time of the incident, the circumstances of the personal data breach, the nature and content of the personal data compromised, the technical and organisational measures applied by the provider to the affected personal data and the relevant use of other providers. Further technical information that must be provided pertaining to the personal data breach includes a summary of the incident, the number of subscribers or individuals concerned, the potential consequences, and the technical and organisational measures taken by the provider to mitigate potential adverse effects. Similar information must be provided to the subscriber or individual.

The Electronic Communications Networks and Services (General) Regulations (SL 399.28) provide that where there is a significant risk of a breach of security or integrity of the services or network, the provider must appropriately and without undue delay notify the Malta Communications Authority (MCA) and any users concerned at the least of the risk and remedies possible, as well as contact points for more information. Serious and significant breaches or failures of international connectivity must be notified to the MCA, and where appropriate, the MCA shall inform regulatory authorities in other member states and the European Network Information Security Agency (ENISA).

Additionally, reporting obligations arise under the Prevention of Money Laundering and Funding of Terrorism Regulations (SL 373.01). Subject persons under these Regulations and the enabling Act are bound to

wh·partners
ADVOCATES & SOLICITORS

Olga Finkel **olga.finkel@whpartners.eu**
Robert Zammit **robert.zammit@whpartners.eu**

Level 5 Quantum House
75 Abate Rigord Street
Ta' Xbiex XBX 1120
Malta

Tel: +356 20925100
Fax: +356 20925902
www.whpartners.eu

report any transaction that they know, suspect or have reasonable grounds to suspect may be related to money laundering or terrorist financing, and must examine with special attention any complex or large transactions or any other behaviour that appear to be suspicious and these findings must be reported to the Financial Intelligence Analysis Unit.

29 What is the timeline for reporting to the authorities?

Under the Commission Regulation 611/2013, all personal data breaches must be reported to the competent national authority no later than 24 hours after the detection of the breach. Providers may give further details of the breach within three days of the initial notification in the event that full details cannot be provided at the time of initial notification.

Reporting obligations under the Prevention of Money Laundering and Funding of Terrorism Reports must be submitted to the Financial Intelligence Analysis Unit (FIAU) as soon as is reasonably practicable, but not later than five working days from when facts are discovered or information is obtained. This time frame may only be waived if the subject person makes representations to the FIAU justifying the reasons why the information cannot be submitted within the said time, and the FIAU may at its discretion extend such time as is reasonably necessary to obtain and submit the information requested.

The reporting obligation in the remote gaming sector is within 24 hours of the incident.

30 Describe any rules requiring organisations to report threats or breaches to others in the industry, to customers or to the general public.

The European Commission Regulations 611/2013 impose an obligation upon electronic communications providers to make a notification of a personal data breach to the subscriber or individual concerned. This notification must be made when the breach is likely to adversely affect the personal data or privacy of the person involved; this notification is made in addition to the notification that must be made to the national competent authority. The notification obligation to the subscriber or individual may only be waived if the technological implementations rendering the data concerned unintelligible to an unauthorised person are to the satisfaction of the competent national authority.

The Electronic Communications Networks and Services (General) Regulations (SL 399.28) provide that where there is a significant risk of a breach of security or integrity of the services or network, the provider must appropriately and without undue delay notify any users concerned at the least of the risk and remedies possible, as well as contact points for more information. Where the MCA determines that the network security breach is in the public interest, it may inform the public of this, or require the undertaking concerned to do so accordingly.

Mexico

Federico de Noriega Olea and Rodrigo Méndez Solís

Hogan Lovells BSTL, SC

Legal framework

1 Summarise the main statutes and regulations that promote cybersecurity. Does your jurisdiction have dedicated cybersecurity laws?

In Mexico there are no dedicated laws that regulate cybersecurity nevertheless, this matter is regulated under the following legislation:

- the Political Constitution of the United Mexican States (the Mexican Constitution);
- the Federal Law on Telecommunications and Broadcasting (FTBL);
- the Federal Law on the Protection of Personal Data Held by Private Parties (the Data Protection Law), its Regulations, Recommendations, Guidelines, and similar regulations on data protection;
- the Federal Law on Transparency and Access to Governmental Public Information, its Regulations and Guidelines;
- the Federal Law of Records, its Regulations and Guidelines;
- the Commerce Code, its Regulations regarding to Certificaction Service Providers;
- General Standards as the Mexican Official Standard Regarding to the Requirements that shall be Observed when Keeping Data Messages;
- the Law on Negotiable Instruments and Credit Operations;
- the Mexican Federal Tax Code;
- the Credit Institutions Law;
- Sole Circular for Banks;
- the Industrial Property Law;
- the Copyright Law;
- the Federal Criminal Code;
- the National Security Law;
- the Federal Labour Law;
- the Federal Law for the Federal Police;
- the National Development Plan 2013–2018;
- the National Program of Public Security 2014–2018;
- the National Program of Security 2014–2018;
- the National Digital Strategy;
- the MAAGTICSI Decree; and
- the Scheme of Interoperability and of Open Information of the Federal Public Administration.

2 Which sectors of the economy are most affected by cybersecurity laws and regulations in your jurisdiction?

Cybersecurity laws mostly affect the financial and telecommunications sectors. Banking institutions have developed diverse mechanisms against cybercrimes in order to protect customers' financial information.

Notwithstanding the above, further efforts are required to raise customers' awareness about the most common cybercrimes and the ways to stop them. Public prosecutors in Mexico are empowered to receive complaints and investigate cyberactivities that may constitute a cybercrime; likewise, the Ministry of Public Security of Mexico City has created the cyber police, which have the responsibility of monitoring any crimes or unlawful activities committed through the internet. Complaints directed to the cyber police can be submitted via its website, phone, twitter account, or e-mail.

3 Has your jurisdiction adopted any international standards related to cybersecurity?

No. Mexico has not yet adopted international standards related to cybersecurity. Nevertheless, the Data Protection Authority in Mexico (INAI), under a formal study named 'Functional Equivalences Table between Security Standards and the Data Protection Law, its Regulations and the Recommendations in Security of Personal Data', assessed more than 20 international standards in order to provide a guide to data controllers and data processors in Mexico, and to evaluate whether the development of any of the privacy and information security international standards analysed would facilitate compliance with the requirements and obligations provided by the Data Protection Law.

In this study the INAI considered that the following international standards comply with the provisions stated in the Data Protection Law by 87 per cent (or more):

- ISO/IEC 27001 (2005, 2013), Information Technology – Security techniques – Information security management systems – Requirements;
- ISO/IEC 27002 (2005, 2013), Information Technology – Security techniques – Code of practice for security management;
- ISO/IEC 29100:2011, Information Technology – Security techniques – Privacy framework;
- ISO/IEC 20000-1:2011 Information technology – Service – management – Part 1: Service management system requirements;
- ISO Guide 72, Guidelines for the justification and development of management systems standards;
- ISO 9000:2005, Quality management systems – Fundamentals and vocabulary;
- BS 10012:2009 Data Protection – Specification for a personal information management system;
- Generally Accepted Privacy Principles (GAPP) from the American Institute of CPAs;
- Control Objectives for Information and Related Technology (COBIT 4.1);
- Control Objectives for Information and Related Technology (COBIT 5); and
- the US Health Insurance Portability and Accountability Act (HIPAA).

4 What are the obligations of responsible personnel and directors to keep informed about the adequacy of the organisation's protection of networks and data, and how may they be held responsible for inadequate cybersecurity?

There are no specific laws in Mexico related to cybersecurity responsibilities or liabilities of personnel and directors. Nevertheless, and in accordance with the Data Protection Law, every private party, individual or organisation that process personal information (data controller), has the obligation to appoint a data person or department (data protection officer) who will be a representative for the organisation in privacy and data protection matters and in charge within the organisation of the correct processing of personal data (including verification of security measures), as well as of processing requests from data owners for the exercise of their rights to access, rectification, suppression or rejection.

In relation to information security, data protection officers shall adopt measures to guarantee due processing of personal data, privileging the interests of the data owners and their reasonable expectation of privacy.

The measures that the data protection officer shall adopt, and that may be related to cybersecurity, include the following:

- issuing policies and programmes, which shall be mandatory within the organisation;
- implementing training programmes;
- implementing a monitoring and surveillance system and internal or external audits to verify compliance with privacy policies;
- assigning resources to the implementation of programmes and policies related to privacy;
- implementing a risk-detection programme to identify privacy risks when launching new products, services, technologies and business models as well as risk-mitigation strategies;
- periodically reviewing security policies and programmes to determine whether amendments are needed;
- performing compliance checks, and
- implementing personal-data tracking systems to trace which data are collected and where they are stored.

Likewise, the data protection officer may have the following duties (focused on cybersecurity):

- monitoring legal and regulatory developments;
- designing policies or practices to protect personal data;
- aligning policies with the business of the organisation;
- monitoring and evaluating internal process for the collection, use, exploitation, storage, suppression and transfer of personal data;
- ensuring legal compliance; and
- training employees in policies and practices with respect to personal data.

The Data Protection Law does not provide a specific sanction for data protection officers, responsible personnel and directors, but it provides that criminal liability may be found (within an organisation) in the event of illegal handling of personal data, whenever:

- any person who is authorised to handle personal information, with the intent to obtain a financial gain, causes the breach of security of the data bases under his or her custody; and
- any person with the intent of obtaining a financial gain, handles personal data through deceit, taking advantage of the errors of or misleading the data owner or the data controller.

5 How does your jurisdiction define cybersecurity and cybercrime?

'Cybersecurity' is defined in the Scheme of Interoperability and of Open Information of the Federal Public Administration as: 'the application of a process of analysis and risk management, related to the use, processing, storage, and transmission of information, as well as with the systems and process used for such purposes, that allow to identify a situation of risk that is known and controlled.'

On the other hand, there is no definition (in statute or case law) of the term 'cybercrime'. Mexico's Federal Criminal Code regulates diverse illegal conducts committed through electronic means (cyberactivities) that could be catalogued as cybercrimes by the use of electronic means for their commission.

Data privacy is regulated (but not itself defined) under the Data Privacy Law.

The distinction between cybersecurity and data privacy in Mexico is that the latter is limited to personal data information and its processing whereas cybersecurity includes all the information (including personal data) that is transmitted through electronic means.

6 What are the minimum protective measures that organisations must implement to protect data and information technology systems from cyberthreats?

As mentioned above, owing to the absence of a specific law that regulates cybersecurity in Mexico, there are no minimum protective measures that organisations must implement to protect data and information technology systems from cyberthreats.

Nevertheless, the Data Privacy Law provides that data controllers have to implement diverse technical, physical and organisational measures in order to protect information against damage, loss, alteration, destruction, use, or unauthorised access or processing.

In this regard, on 30 October 2013 the INAI issued the 'Recommendations on Security of Personal Data' and expressed as a general recommendation to adopt a Security Management System of Personal Data, which the INAI has defined as a:

> *general management system to establish, implement, operate, monitor, review, maintain and improve processing and security of personal data on the basis of the risk of the assets and of the basic principles of legality, consent, information, quality, purpose, loyalty, proportionality and liability provided for in the Data Protection Law, its regulations, secondary regulations and any other principle which provided good international practice in the matter.*

In addition to the foregoing, there are certain specific mandatory security measures that certain industries must adopt to protect their customers' data. This is particularly true in the banking and financial sectors. Banking laws and regulations provide that banks must implement certain security measures in electronic banking transactions and require the use of several passwords depending on the amount and nature of the transaction.

7 Does your jurisdiction have any laws or regulations that specifically address cyberthreats to intellectual property?

The Federal Criminal Code regulates in its Title 26 conducts committed against intellectual property and copyrighted material. Specific provisions related to cyberthreats provide criminal penalties for those persons who use, reproduce, distribute, store, sell, lease, among other conducts, copyrighted material, in a malicious way, seeking financial gain and without the corresponding authorisation.

Likewise, the action of manufacturing a system or equipment with the purpose of making a profit and focused on voiding electronic means of software protection will be penalised.

8 Does your jurisdiction have any laws or regulations that specifically address cyberthreats to critical infrastructure or specific sectors?

The Federal Criminal Code regulates as the crime of sabotage the damage, destruction or harming of, or unlawful interference with, roads, public services, or state services; steel, electric or basic industries; centres of production or distribution of weapons, ammunition or military equipment, with the aim of disrupting the economic life of the country or affect their ability to defence. On the other hand, the Federal Criminal Code also protects means of communication such as telegrams, telephone lines, radio communications, telecommunication networks, as any component of an installation of production of magnetic or electromagnetic energy or its means of transmission.

Regarding telecommunications, article 426(I)(II) of the Federal Criminal Code provides that persons who manufacture, import, sell or lease any device or system, or commit any act with the purpose of decoding any encrypted protected satellite signal without the legitimate authorisation of the licensed distributor, will be imposed six months to four years' imprisonment and a fine of 300 to 3,000 days of the general minimum wage in Mexico City (approximately €1,200 to €12,000).

In this regard the Law on Negotiable Instruments and Credit Operations sanctions diverse actions that affect any kind of financial payment instruments (eg, credit or service cards) or the information contained on them. Likewise, this law sanctions the following conducts:

- the alteration, copy or reproduction of the magnetic band of payment instruments or any other technical identification method contained on them;
- acquiring, possessing, use or commercialising of equipment or electronic means (or any kind of technology means) to remove, copy or reproduce information contained on financial instruments in order to obtain economic resources or confidential information; and
- the unauthorised access to equipment or electronic means used by financial institutions or the alteration or modification of the physical equipment or electronic means that are used for cash withdrawal (ATMs).

By interpretation of this law, the authority may consider as committed through a cyberthreat any of the conducts mentioned above and impose a corporal penalty from three to nine years' imprisonment and a fine of 30,000 to 300,000 days of the general minimum wage in Mexico City (approximately €120,000 to €1.2 million). Where the offender is a director, officer, employee or service provider of a financial institution, such penalties or fines will be increased by half that amount again.

At the time of writing, the general minimum wage in Mexico City is currently 70.10 pesos.

9 Does your jurisdiction have any cybersecurity laws or regulations that specifically restrict sharing of cyberthreat information?

The Mexican Constitution was amended on 1 July 2009, affecting one of its main provisions regarding privacy rights. The provision amended was article 16, which provides that:

> *[n]o one may be subjected to interference with his or her person or his or her family, domicile, documents or possessions, except in accordance with a written order from the competent legal authority, in due form and for reasons previously defined by the law [...]*

According to the above-mentioned constitutional provision, every intrusion of personal property or possessions has to be legally supported by a prior judicial order or warrant.

Confidentiality of communications is protected under the Federal Code of Criminal Procedures (FCCP), which in its Chapter VIII-bis related to the Private Communications between Private Parties article 278-bis and ter provides that communications between private persons may be provided as a proof in a criminal trial or procedure when such communications have been obtained by the party itself, or with the support of the authority, in other words, by a judicial order.

Likewise, the FCCP provides the obligation to concessionaries and authorised companies of telecommunications or internet service providers to collaborate with authorities in obtaining such proofs. In this regard the FTBL provides a specific Title that regulates the provision of private information to competent authorities for criminal investigation and prosecution.

Information requests that require the intervention of an authority for the interception of private communications shall be made by an individual party before the Attorney-General of the Republic or the corresponding empowered public servant, so the judicial authority may validate the existence of sufficient evidence that could support the need for a criminal investigation.

The Law Against Organised Crime provides that in the investigation of a crime in which it is assumed on good grounds that a member of the organised crime is involved, it is possible to tap private communications. It also provides for the obligation of concessionaires, permissionaires and any person holding equipment or a system that could be intercepted, to cooperate with the authorities, prior to a judicial order.

The Law to Prevent and Sanction Kidnapping Crimes provides the possibility to tap private communications by using any technological means deemed necessary for such purpose, and the obligation of public telecommunications network concessionaires' and companies that commercialise telecommunication services to cooperate with the authorities and perform certain actions.

10 What are the principal cyberactivities that are criminalised by the law of your jurisdiction?

There are diverse cyberactivities criminalised by the Mexican Federal Criminal Code. With regard to organisations, the following cybercrimes are the most relevant: espionage; conspiracy; crimes against means of communication; tapping of communications; violation of the secrecy of correspondence; acts of corruption; breach of confidence (disclosure of secrets); non-authorised access to computer systems; document falsification; threats against peace and security; fraud; extortion; and operations using illegal resources (money laundering).

11 How has your jurisdiction addressed information security challenges associated with cloud computing?

The Data Protection Law regulates the provision of services over the cloud. It provides that data controllers shall verify, prior to contracting a cloud computing service, that the service provision by the data processor:

- has and applies data protection policies according to the Data Protection Law and its Regulations;
- fully informs about the services subcontracted;
- does not include conditions in the service provided that assume that the ownership of the data could be transferred; and
- keeps personal data confidential.

Likewise, the data processor must have mechanisms that:

- make the contracting party aware about changes to its privacy policies or the terms and conditions of the service provided;
- allow the data control to limit the processing of personal data;
- implement security measures for data protection;
- guarantee that personal data will be deleted at the end of the service contracted; and
- do not allow access to personal data to unauthorised persons and inform the data controller when an authority requests access to such data.

12 How do your jurisdiction's cybersecurity laws affect foreign organisations doing business in your jurisdiction? Are the regulatory obligations the same for foreign organisations?

In general, obligations are the same for domestic and foreign organisations. We do not identify a barrier for foreign companies that want do to business in Mexico. The absence of specific security measures and technologies give foreign and domestic companies flexibility on the security measures they adopt.

Best practice

13 Do the authorities recommend additional cybersecurity protections beyond what is mandated by law?

In accordance with the Data Protection Law, binding self-regulation schemes may be adopted by data controllers in order to comply with and complement the provisions stated in data privacy regulations in Mexico. Self-regulation may include codes of ethics or good practice, privacy policies, binding corporate rules or other mechanisms that harmonise data processing performed by self-regulated entities and that facilitate the exercise of data owners' rights.

In this regard, the INAI issued the 'Recommendations on Security of Personal Data', described in question 6.

14 How does the government incentivise organisations to improve their cybersecurity?

There is not a specific incentive to organisations to improve their cybersecurity, nevertheless, some provisions may be found in the Data Protection Law, and when a data controller adopts and complies with a self-regulation scheme; the foregoing action will be taken into consideration by the INAI when imposing penalties or sanctions for the breach of the Data Protection Law or its Regulations.

15 Identify and outline the main industry standards and codes of practice promoting cybersecurity. Where can these be accessed?

Mexican industry standards and codes of practice promoting cybersecurity are not regulated or publicly available. As it is considered as a self-regulated activity, its publicity is not a practice implemented in Mexico. Recently, in September 2015, the International Chamber of Commerce Mexico published the ICC Cybersecurity Guide for Business, which is a tool and self-regulatory guidance to promote good business practice. Such guide may be found and downloaded at http://phrenesis.net/ICC-Cyber-security-guide-for-business.pdf.

16 Are there generally recommended best practices and procedures for responding to breaches?

In the remote gaming business, the best practices currently in place are the safe-keeping of all data related to the cyberthreat, the setting up of a dedicated team to identify the source of the threat and ensure proper steps are taken to avoid recurrence of such incident, and the education of the employees to ensure that all employees are aware of the threats and the importance of following the company's procedures and policies. Where necessary, third-party firms are engaged to perform penetration tests to ensure that the systems used are adequately secure. Likewise, in the case of a data protection breach of information, the data controller shall immediately notify the data subjects that may be affected significantly on their patrimonial or moral rights and implement a process of an exhaustive review of the incident. In these cases, the data controller shall implement corrective actions in order to prevent another similar breach, provide to the affected data subjects preventive measures and recommendations to protect the information compromised and inform them of the means on

which they will be provided more information about the breach and the progress on its solution.

17 Describe practices and procedures for voluntary sharing of information about cyberthreats in your jurisdiction. Are there any legal or policy incentives?

At present, there do not exist any legal or policy incentives targeting the voluntary sharing of information relating to cyberthreats as such.

18 How do the government and private sector cooperate to develop cybersecurity standards and procedures?

Collaboration agreements are the most common legal instruments by which the Mexican government and private sector cooperate on cybersecurity matters. In May 2014, the Federal Police, which is the authority in charge of cybersecurity in Mexico, signed, with a major IT company, a business cooperation agreement to take actions against cybercrime and unlawful conducts, prevent illegal activities and promote internet security in Mexico.

From 26 to 30 October 2015, the Ministry of the Interior, the National Security Commission, the Federal Police and the Organization of American States organised Cybersecurity Week 2015 in Mexico, during which the 32 Mexican states enacted an agreement of collaboration for exchange of information and obtaining support, training and technical assistance by the Federal Police. Another achievement was the presentation of the 'Cyberpolice Model' by the Scientific Division of the Federal Police. With such model and with its implementation, the Federal Police are seeking to boost the capacities of the government to prevent and investigate cyberthreats, cybercrimes, bring attention to criminal complaints to strengthen the channels of national coordination and generate national statistics of cybercrimes.

19 Is insurance for cybersecurity breaches available in the jurisdiction and is such insurance common?

Few companies in Mexico have been offering a cybersecurity insurance policy protecting against cyberattacks and cybercrimes. In the financial sector, some banks offer customers their support in the case they suffer a cybersecurity threat or if their bank information or funds are compromised. However, insurance policies for cybersecurity breaches, per se, are not yet common in Mexico.

Enforcement

20 Which regulatory authorities are primarily responsible for enforcing cybersecurity rules?

The following authorities are responsible for enforcing cybersecurity rules in Mexico:

- the Attorney-General of the Republic;
- the Public Prosecutor;
- the INAI;
- the Ministry of Communications and Transportation; and
- the Federal Institute of Telecommunications.

21 Describe the authorities' powers to monitor compliance, conduct investigations and prosecute infringements.

In accordance with the Mexican Constitution, a warrant shall be obtained before the Mexican courts to compel any individual or entity to disclose any kind of private information. The authority empowered to order the disclosure of private information is a judge in a specific matter or trial and it may be possible, in certain cases, for a private person to make such a request to a judge.

In general, the following authorities are able to conduct investigations and prosecute infringements:

(i) the Attorney General of the Republic (federal);
(ii) the public officers that have being expressly delegated such power by the Attorney-General of the Republic;
(iii) the State Attorney Generals (local); and
(iv) the authority specialised on the corresponding matter.

Each of the authorities mentioned in (i) to (iii) may perform investigative activities regarding extortion crimes, threats, kidnappings, organised crimes or any other serious crimes, acting on their respective competences.

In the case of data protection, in order to monitor compliance the INAI may conduct investigations to monitor compliance in the processing of personal data in accordance with the provisions stated in the Data Protection Law. In most cases, the Data Protection Authority does not act ex officio. Generally, the authority acts upon a claim by an individual to monitor compliance, conduct investigations and prosecute infringements.

The Mexican Constitution provides that a person's properties and possessions may not be investigated without a judicial order. In accordance with the foregoing, a warrant shall be obtained before the Mexican courts to compel a company to provide documents or persons to participate in interviews related to any kind of incidents or investigations of crimes (including cybersecurity). Only those authorities that have the power of investigation could request or demand documents or interviews related to incidents (including cybersecurity).

22 What are the most common enforcement issues and how have regulators and the private sector addressed them?

Resolutions of administrative proceedings dealing with the imposition of sanctions are published on INAI's website (www.ifai.org.mx). The most significant resolutions were against financial institutions. One of the last sanctions imposed by the INAI reached an amount of approximately €1.8 million. Among others, the following acts are commonly committed by the sanctioned companies:

- process sensitive data without obtaining data subject's consent;
- non-response to protection of rights request;
- acting with negligence in the protection of personal information;
- violation of data protection principles provided in the Data Protection Law;
- illegitimate processing of personal data; and
- collection of financial and economic data without consent.

We have not yet identified any case of imposition of sanctions related to data security breaches. Nevertheless, we noticed that INAI, in 2015, initiated an investigation into a telecommunications company, which had a leak of information of its customers and into a department store, whose systems were hacked leading to the leak of confidential and customers' information.

23 What penalties may be imposed for failure to comply with regulations aimed at preventing cybersecurity breaches?

Fines are approximately from 200 to 320,000 days of the general minimum wage in Mexico City (approximately €800 to €1.3 million) where the INAI resolves that the breach was attributable to a private party by compromising on the security of its databases, sites, programs or equipment. If sensitive data were compromised, the fine may be doubled.

Likewise, the following custodial penalties may be imposed: from three months to three years' imprisonment to any person who, authorised to process personal data and looking to obtain a profit, causes a security breach to databases under his or her custody; and six months to five years' imprisonment to any person who, looking to obtain a profit, processes personal data by misleading or taking advantage of an error that a data owner (or the person authorised for its transmission) incurs.

24 What penalties may be imposed for failure to comply with the rules on reporting threats and breaches?

There is no specific penalty for failure to comply with the rules on reporting threats or breaches; nevertheless, the INAI is legally capable to evaluate if the cause that originated a data breach was caused by a failure of compliance or negligence and, in such cases, the penalties that may imposed range from 200 to 320,000 days of the general minimum wage in Mexico City (approximately €800 up to €1.3 million), and doubled if sensitive data were compromised. Likewise, as mentioned above, and on the same terms as stated, custodial penalties may be imposed.

25 How can parties seek private redress for unauthorised cyberactivity or failure to adequately protect systems and data?

Any data owner may file a claim against a data controller or data processor before the INAI. Even though the law provides that the administrative procedure is in addition to any civil or criminal procedure, it is not clear whether a ruling from the INAI is required prior to commencing a tort

liability action as is the case in other laws that provide administrative procedures and special authorities to survey and penalise infringements.

In accordance with the Federal Civil Code, customers may bring civil actions against a data controller or data processor for damages (including moral damages) that arise as a consequence of the breach of confidentiality obligations.

Threat detection and reporting

26 What policies or procedures must organisations have in place to protect data or information technology systems from cyberthreats?

The legislation is silent with regard to rules and regulations that organisations shall follow in order to protect data or information technology systems from cyberthreats. Best practices and international standards are usually adopted by entities to protect their systems and information.

27 Describe any rules requiring organisations to keep records of cyberthreats or attacks.

There is no provision that requires organisations to keep records of cyberthreats or attacks.

28 Describe any rules requiring organisations to report cybersecurity breaches to regulatory authorities.

There is no regime requiring organisations to notify data breachs to the authorities. Nevertheless, data breaches must be notified to the data owners, but only those that significantly affect their patrimonial or moral rights.

Additionally, in certain cases, filing a criminal complaint with the General Attorney may be advisable if the cyberattack may result in a crime being committed.

29 What is the timeline for reporting to the authorities?

Notice to data owners shall be made immediately after becoming aware of the data breach.

Update and trends

The principal challenge in Mexico is that there is no specific law regulating cybersecurity. To shape a favourable regulatory environment, companies may participate through public consultations or at summits or events organised by the security authorities in Mexico.

In the near future, the Mexican government is looking to implement a National Cybersecurity Model, which will be implemented throughout all of the Mexican states in order to homologate knowledge, protocols and action plans that shall be followed by all the police bodies in the country. Through such model, Mexican authorities will be able to react quickly to cybercrimes to protect the Mexican population.

Considering that Mexico is a country whose online activity is one of the biggest (by 43 per cent of its citizens), on 22 October 2015, a senator proposed a bill of Cybersecurity Law, integrated by 48 articles. This is the first bill of cybersecurity law ever proposed in Mexico. It proposes to consider as criminal offences (cybercrimes) conduct related to the interception and interference of computer systems, use of computer weapons, sexual predation, intimidation and improper disclosure of personal information, activities that affect victims' patrimony, identity theft, attacks and cyberterrorism, cyberespionage, violation of digital seals, correspondence and electronic messages.

30 Describe any rules requiring organisations to report threats or breaches to others in the industry, to customers or to the general public.

The notification must include the nature of the incident, the compromised data, the recommendations to the data owners as to what measures they may take to protect their interests, the corrective actions taken and how data owners can get more information on the matter.

Hogan Lovells BSTL

Federico de Noriega Olea **federico.denoriega@hoganlovells.com**
Rodrigo Méndez Solís **rodrigo.mendez@hoganlovells.com**

Paseo de los Tamarindos 150-PB
Bosques de las Lomas
Cuajimalpa de Morelos
Mexico City 05120
Mexico

Tel: +52 55 5091 0000
Fax: +52 55 5091 0123
www.hoganlovells.com

Norway

Christopher Sparre-Enger Clausen
Advokatfirmaet Thommessen AS

Legal framework

1 Summarise the main statutes and regulations that promote cybersecurity. Does your jurisdiction have dedicated cybersecurity laws?

In Norway, there are currently no dedicated cybersecurity laws. However, a number of laws and regulations regulate various aspects of cybersecurity and information security in general, including requirements applicable to both the public and private sector aimed at promoting cybersecurity. In 2012, the Norwegian government issued a Cyber Security Strategy, whose primary objective is to 'set the direction and priorities that will form the basis for the government's information security efforts in the coming years'. The Cyber Security Strategy is further intended to complement existing legislation and indicate the direction of further development of the legislation concerning cybersecurity. The Cyber Security Strategy contains certain overarching goals for information security (from an information and communication technology perspective) to be operationalised through certain identified strategic priorities, such as the application of systematic measures and security standards, improvement of information and communication technologies (ICT) infrastructure, safeguarding of society's ability to prevent cybercrime and ICT incidents, and efforts to raise awareness and competence with respect to cybersecurity. In November 2015, the Committee of Digital Vulnerability submitted its report in the form of an official Norwegian Report to the Ministry of Justice and Public Security. The report describes digital vulnerabilities that Norway faces at present and in the near future, and assesses the consequences this vulnerability may have for individuals, businesses and industries and civil protection. The report sets out proposals on specific measures to be implemented within the different business sectors in order to prevent information from being processed unlawfully or compromised in other ways. The report also recommends a series of concrete amendments to the current infrastructure and to the authorities who govern them.

Within the current legislative framework, the promotion of cybersecurity (and prevention of cybercrime) is addressed, directly or indirectly, in the following laws and regulations.

The Norwegian Personal Data Act (NPDA) dated 14 April 2000 is an important source of law with respect to promoting cybersecurity. The purpose of the NPDA is to protect natural persons against violation of their right to privacy through the processing of personal data, and shall help to ensure that personal data are processed in accordance with fundamental respect for the right to privacy, including the need to protect personal integrity and private life and ensure that personal data are of adequate quality. The NPDA and the Norwegian Personal Data Regulations (NPDR) include general provisions relating to data and information security where personal data are processed.

A number of detrimental cyberactivities are criminalised by the Norwegian Penal Code dated 20 May 2005. The Penal Code of 2005 took effect from 1 October 2015 and replaces the previous General Civil Penal Code of 1902. Such crimes include unlawful access to data (data breach), vandalism in the form of unlawful tampering with someone else's data, making available passwords or other access data, disk operating system (DoS) attacks, unlawful use of computing power and identity theft.

For some sectors, specific requirements with regard to security apply. The Electronic Communications Act dated 4 July 2003 (ECA) and the Electronic Communications Regulations (ECR) include special provisions for security and preparedness applicable to providers of electronic communications services. Please note that the European Network and Information Security Agency regulation (Regulation (EU) No. 526/2013) has been implemented into Norwegian law by reference in the ECR (section 8-7). The Norwegian Post and Telecommunications Agency (an autonomous agency of the Ministry of Transport and Communications) is responsible for the supervision and enforcement of the ECA and the ECR.

For financial institutions, the ICT Regulations dated 21 May 2003 set out provisions for security requirements for the institutions' ICT activities, risk analysis, etc. The Regulations relating to Preventive Security and Preparedness in the Energy Supplies dated 7 December 2012 include provisions on, inter alia, information security in the energy sector for entities that are comprised by the nationwide Power Supply Preparedness Organisation (KBO). For the offshore sector, the Petroleum Activities Act dated 29 November 1996 includes a provision requiring licensees to initiate and maintain security measures to contribute to avoiding deliberate attacks against facilities and have contingency plans to deal with such attacks (such as espionage and sabotage).

The eGovernment Regulations dated 25 June 2004 apply to the entire public sector and impose obligations on public agencies to use information security management systems.

The Act relating to Protective Security Services (the Security Act) dated 20 March 1998 aims to take steps enabling the effective countering of threats to the independence and security of the realm and other vital national security interests and to set out provisions relating to, inter alia, information security for this purpose. The Security Act applies to the entire public sector (ie, administrative agencies) as well as certain suppliers of goods or services to administrative agencies, and, in some cases, any other legal person who owns or otherwise controls or supervises a 'sensitive object' or who is granted access to classified information by an administrative agency.

2 Which sectors of the economy are most affected by cybersecurity laws and regulations in your jurisdiction?

The public sector, the telecommunications sector, the IT sector, the financial sector and the oil and energy sector are generally most affected by cybersecurity laws and regulations in Norway.

In Norway, cyberattacks against online banks started becoming a serious threat in 2007. During December 2007, the online banks of two Norwegian banks were attacked by Trojans at the same time and the number of attacks has only increased in the following years. In 2014, several Norwegian banks and other large corporations were hit by a DoS attack that lasted several hours. The consequences were mainly economic loss as well as downtime for the systems involved. The many cyberattacks within the financial sector resulted in the formation of FinansCERT, a Norwegian cyber crime unit for the financial sector, in 2013. FinansCERT serves banks, life insurance and pension companies that are members of Finance Norway and represents a joint cooperation to fight cyber crimes against the financial sector.

Notably, during the summer of 2014, the Norwegian National Security Authority reported on the most extensive hacking attack ever against the oil and energy sector by the use of 'spearphishing' (phishing attempts directed at specific individuals or companies). In 2013, the largest telecommunications company in Norway was the target of a similar attack.

3 Has your jurisdiction adopted any international standards related to cybersecurity?

The Norwegian government has, as a part of its Cyber Security Strategy, recommended that all public and private companies apply a more systematic approach to cybersecurity, including the application of recognised standards in the use of information security management systems. In particular, the Agency for Public Management and eGovernment (Difi) recommends that public activities are based on ISO/IEC 27001:2013 when establishing information security management systems. The recommendation from Difi is intended to give the relevant entity the necessary scope of action for the use of the standard depending on the distinctive aspects, risks and materiality relating to each entity.

4 What are the obligations of responsible personnel and directors to keep informed about the adequacy of the organisation's protection of networks and data, and how may they be held responsible for inadequate cybersecurity?

The general manager will normally be responsible for the day-to-day management of the company's activities, and will in this capacity be responsible for ensuring that the organisation's networks and data are adequately protected. The general manager and members of the board of directors may be held liable for damages or loss caused by such individuals' negligence or wilful misconduct in performing their duties for the company, pursuant to the Private Limited Liability Companies Act and the Public Limited Liability Companies Act of 13 June 1997 (directors' and officers' liability). Presumably, such liability may for instance be relevant in circumstances where the general manager or the board of directors, or both, have neglected obvious cybersecurity threats or otherwise omitted, wilfully or negligently, to implement adequate cybersecurity measures.

Pursuant to the NPDR, the general manager is responsible for ensuring compliance with the relevant data security requirements. A similar provision is included in the Regulations on Preventive Security and Preparedness in the Energy Supply, pursuant to which the general manager for the relevant entity is responsible for ensuring compliance with the relevant provisions of the Regulations.

5 How does your jurisdiction define cybersecurity and cybercrime?

There are no statutory or case law definitions of cybersecurity and cybercrime in Norway.

As part of the revision of the penal provisions in the Norwegian General Civil Penal Code relating to protection of information and information exchange, it was concluded that it was not necessary to give the term 'cybercrime' a legal definition. The preparatory works state, however, that the term 'cybercrime' following a common understanding comprises both crimes that are directed against computers and computer systems, and crimes where computer equipment is used as a tool to commit the action (ie, crimes that are connected with the use and utilisation of ICT).

In the Norwegian Ministry of Government Administration, Reform and Church Affairs report to the Stortinget (White Paper), Meld.St.23 (2012–2013), 'Digital Agenda for Norway – ICT for Growth and Value Creation', it is stated that 'cybercrime' is a generic term for various types of criminal activity, either using ICT tools to commit crimes or committing criminal acts involving computer data and computer systems. The report mentions crimes for profit such as e-commerce fraud, identity fraud, denial of service (DoS) attacks, illegal access, damaging important information systems or infrastructure, and cyberespionage as examples of cybercrime.

The Cyber Security Strategy prepared by the government in 2012 defines cybersecurity as 'protection of data and systems connected to the internet', and is otherwise generally referred to as a subcategory of 'information security'.

In many aspects, the terms cybersecurity and data privacy overlap as the NPDA and NPDR set out detailed requirements with regard to data security. However, the term data privacy relates only to personal data (ie, information and assessments that may be linked to a natural person), whereas the term cybersecurity not necessarily is limited to security aspects where personal data are processed.

6 What are the minimum protective measures that organisations must implement to protect data and information technology systems from cyberthreats?

Pursuant to the NPDA, organisations shall, by means of planned, systematic measures, ensure satisfactory data security with regard to confidentiality, integrity and accessibility in connection with the processing of personal data.

For organisations within certain sectors, such as the public sector, telecommunications sector and the health sector, specific regulations and statutory requirements may apply with respect to protective measures.

Pursuant to the Security Act and the Information Security Regulations, there are specific and comprehensive requirements with regard to information security in administrative agencies and other legal persons to whom the Act applies. Before sensitive information is processed, stored or transmitted in an information system, the National Security Authority shall approve the system for the security classification concerned. Further, only cryptosystems that have been approved by the National Security Authority are allowed to be used to protect sensitive information in administrative agencies or other legal persons to whom the Act applies. The National Security Authority shall also approve crypto-algorithms that are used in equipment intended for export.

7 Does your jurisdiction have any laws or regulations that specifically address cyberthreats to intellectual property?

The Norwegian Copyright Act dated 12 May 1961 includes new provisions (effective as of 2013) relating to special measures in the event of infringement of copyright, etc on the internet.

If it is substantiated that copyright is infringed as part of, for example, file sharing, the owner of the copyright may, following a concrete assessment, request the courts to order internet service providers (ISP) to reveal information that identifies the owner of the subscription used in the infringement, for example who is the holder of a specific IP address. This will enable the owner of the copyright to take further steps against the infringer, which otherwise would be difficult because the ISPs are subject to legal secrecy.

The owner of a copyright may also request the courts to impose certain providers of information society services (such as services consisting of providing access to or transmitting information via an electronic communication network or of hosting information provided by the recipient of a service) to block or impede the access to websites on which material that obviously infringes copyright is made available on a large scale. The court will have to consider whether the reasons that suggest that such order shall be given outweigh the disadvantage the order will result in, also taking into consideration, inter alia, the freedom of information and freedom of speech.

8 Does your jurisdiction have any laws or regulations that specifically address cyberthreats to critical infrastructure or specific sectors?

The Regulations relating to Preventive Security and Preparedness in the Energy Supplies dated 7 December 2012 include provisions on, inter alia, information security in the energy sector for entities that are comprised by the nationwide KBO. Pursuant to the regulations, all information that is sensitive to the energy supplies (ie, specific and thoroughgoing information with regard to the energy supplies, which may be used to harm plants or affect functions of importance for the energy supplies) shall be identified and be subject to routines for protection, shielding and access control.

All energy entities that have production control systems shall at all times protect the production control system against all kinds of unwanted incidents, including all types of unauthorised access in order to prevent misuse and distribution of malicious software and similar. The entity shall have control measures for awarding, alteration, deleting and assessing correct access to the production control system. The entity shall at all times be able to control or monitor the personnel that are or have been logged in to the production control system, and also whether external connection is used. Specific requirements apply for equipment used in the production control system. Restrictions apply for external connection to the production control system.

For financial institutions, the ICT Regulations dated 21 May 2003 set out provisions for security requirements for the institution's ICT activity. With regard to security, the institutions shall prepare procedures for ensuring that equipment, systems and data of significance for the institution's business are protected against damage, misuse, unauthorised access and change, and vandalism. The procedures shall also contain guidelines for the granting, modification, revocation and control of access to the ICT systems. As far as is practicable, security requirements shall be quantifiable. Fulfilment of the requirements for protection of personal data under the NDPR shall be regarded as fulfilment of these requirements.

Within the telecommunications sector, the ECA and the ECR impose obligations on providers of electronic communications services to implement necessary security measures for the protection of communications and data in the provider's networks and services (ECA section 2-7), as well as general obligations to provide adequate security and maintain necessary preparedness within the network at all times (ECA section 2-10). Further, the ECR contains requirements for the providers to prepare plans and take measures to maintain an adequate security level within their respective networks. The Post and Telecommunications Agency has been given certain powers to instruct providers to present plans and participate in preparedness exercises.

9 Does your jurisdiction have any cybersecurity laws or regulations that specifically restrict sharing of cyberthreat information?

Generally, the recording or accessing of private communications is prohibited under the Norwegian Penal Code. The law enforcement agencies have a certain right to lawfully intercept electronic communication and conduct communications control in connection with the investigation of criminal offences pursuant to the Criminal Procedures Act dated 22 May 1981. There are no specific laws governing access to metadata.

10 What are the principal cyberactivities that are criminalised by the law of your jurisdiction?

Norwegian law enforcement agencies have over recent years increased their efforts to prevent and fight cybercrime. The principal cyberactivities that are criminalised under Norwegian law, and which are relevant to organisations, are:

- data breach: it is illegal to unlawfully obtain data or software that are stored or transferred by electronic or other technical means. Violations are punishable by fines or imprisonment for a term not exceeding six months, or both;
- vandalism: acts consisting of unlawful changing, additions to, damaging of, deleting or concealing of someone else's data are considered as vandalism and punishable by fines or imprisonment of up to one year;
- DoS attacks: attempts to make a machine or network resource unavailable to its intended users by transferring, damaging, deleting, depreciate, change, adding or removing information are punishable by fines or imprisonment of up to two years;
- unlawful production, acquisition, possession or distribution of passwords or other access data that may give access to a computer system is punishable by fines or imprisonment of up to one year;
- unlawful production, acquisition, possession or distribution of a software program or device specifically engineered to commit a cybercrime, such as computer viruses, hacker software or similar, is punishable by fines or imprisonment of up to one year;
- unlawful use of computing power is punishable by imprisonment of up to three years;
- unlawful interception: unlawfully obtaining data or software that are stored or transferred by electronic or other technical means is punishable by fines or imprisonment of up to six months; and
- computer fraud: fraud by altering data or software or otherwise unlawfully influencing the result of automatic data processing is punishable by fines or imprisonment of up to three years.

11 How has your jurisdiction addressed information security challenges associated with cloud computing?

The Norwegian Data Protection Authority has published guidelines for the use of cloud computing services. With regard to information security, the Data Protection Authority points to the fact that the data controller shall carry out a risk assessment for its processing of personal data. The risk assessment must be seen in conjunction with established risk acceptance criteria, and the controller shall implement appropriate measures to achieve satisfactory information security.

12 How do your jurisdiction's cybersecurity laws affect foreign organisations doing business in your jurisdiction? Are the regulatory obligations the same for foreign organisations?

In most aspects, the regulatory obligations will be the same for foreign organisations doing business in Norway.

In particular, the NPDA applies to (i) controllers who are established in Norway, and (ii) controllers who are established outside the territory of the EEA, but who make use of equipment in Norway. However, the latter shall not apply if such equipment is used only to transfer personal data through Norway. Controllers such as those mentioned under (ii) must have a representative who is established in Norway, in which case the provisions of the NPDA that apply to the controller shall also apply to the representative.

The ICT Regulations apply to Norwegian financial institutions (such as commercial banks, savings banks, finance companies, insurance companies, etc), depending on whether the institutions are subject to the relevant regulatory regimes in Norway.

The Security Act applies to any organisation that is a supplier of goods or services to a Norwegian administrative agency in connection with a classified procurement.

The ECA applies to electronic communications and associated equipment in Norway, as well as to Norwegian ships and aircraft and to installations and devices of whatever nature connected to petroleum activity on the continental shelf or for utilisation of renewable energy resources at sea within the scope of the Norwegian Offshore Energy Act.

The Norwegian General Civil Penal Code applies to criminal acts committed in Norway. In cases in which the criminality of an act depends on or is influenced by any actual or intended effect, the act shall be regarded as committed also where such effect has occurred or is intended to be produced. This means, for example, that cybercrimes committed via the internet where the offender makes use of computer equipment abroad and the effect occurs in Norway are likely to be caught by the Penal Code. Further, most cybercrimes will also be punishable in Norway if the act is committed abroad by any Norwegian national or any person domiciled in Norway, or abroad by a foreign national when the act is a felony also punishable according to the law of the country in which it is committed and the offender is resident or staying in Norway.

Best practice

13 Do the authorities recommend additional cybersecurity protections beyond what is mandated by law?

In the Cyber Security Strategy for Norway issued in 2012, the government has recommended all public and private companies to apply recognised standards in the use of information security management systems in order to safeguard information security comprehensively and systematically. The government points out that the requirements must be tailored to the risk facing the individual organisation. The nature, size and social significance of the organisation will dictate its level of ambition and allocation of resources to security efforts.

14 How does the government incentivise organisations to improve their cybersecurity?

The Norwegian government has not introduced any specific incentive programmes or similar to improve cybersecurity, but several initiatives are being discussed as part of the public debate on cybersecurity.

15 Identify and outline the main industry standards and codes of practice promoting cybersecurity. Where can these be accessed?

See question 3. Both the Agency for Public Management and eGovernment (Difi), IKT Norge and the Norwegian Computer Association continue to provide guidance and recommendation on standards and codes of practice with a view to improving cybersecurity awareness and capabilities. See the relevant website for further information (www.ikt-norge.no/, www.data-foreningen.no/ or www.difi.no/).

16 Are there generally recommended best practices and procedures for responding to breaches?

We are not aware of any generally recommended best practices and procedures for responding to breaches other than what follows from legal obligations.

17 Describe practices and procedures for voluntary sharing of information about cyberthreats in your jurisdiction. Are there any legal or policy incentives?

As far as we are aware, there are no established practices and procedures for voluntary sharing of information about cyberthreats other than what follows from the legal obligations.

18 How do the government and private sector cooperate to develop cybersecurity standards and procedures?

In Norway, the key national cybersecurity stakeholders have initiated a partnership to establish the Centre for Cyber and Information Security (CCIS), a national centre for research, training, and education in cyber- and information security. Both the private and the public sector contribute in this initiative, including, for example, educational institutions, law enforcement agencies, large IT corporations and power supply organisations. Companies can contact and interact with the CCIS and its collaborative partners to, among other things, discuss current and potential challenges pertaining to cybersecurity.

19 Is insurance for cybersecurity breaches available in the jurisdiction and is such insurance common?

Several insurance companies offer crime insurance to businesses. These insurance policies may normally be expanded to include cybercrime insurance. Cybercrime insurance covers financial losses inflicted by third parties (ie, persons other than those who work in the business) committing offences through the organisation's computer systems.

Enforcement

20 Which regulatory authorities are primarily responsible for enforcing cybersecurity rules?

The Norwegian Data Protection Authority is responsible for enforcing the NPDA and NPDR.

The Norwegian Water Resources and Energy Directorate (NVE) is responsible for enforcing the special information security provisions included in the Regulations relating to Preventive Security and Preparedness in the Energy Supplies.

The Financial Supervisory Authority of Norway is responsible for enforcing the ICT Regulations that apply to financial institutions.

The Norwegian Post and Telecommunications Authority monitors compliance with the ECA.

The Norwegian National Security Authority shall control the security status of the enterprises to which the Security Act applies (ie, it ensures that the security provisions of the Act on protective security services are complied with).

All criminal prosecution is conducted by the law enforcement agencies.

21 Describe the authorities' powers to monitor compliance, conduct investigations and prosecute infringements.

The Norwegian Data Protection Authority and the Privacy Appeals Board may demand any data necessary to enable them to carry out their functions. In addition, the Data Protection Authority may carry out such tests or inspections as it deems necessary and may demand such assistance from the personnel in such places as is necessary to carry out the tests or inspections (eg, by interviews).

The Post and Telecommunications Authority may demand information that is necessary for the implementation of the ECA, decisions made pursuant to the ECA, or obligations resulting from international agreements to which Norway has become a party. On request from the Authority, providers shall submit information, including classified information on electronic communications networks and services and on infrastructure connected to the operating and control systems. The duty of confidentiality for providers and installers does not preclude the duty to provide information. The Authority may issue orders to correct or cease unlawful activities and lay down conditions that must be met for the activity to be in accordance with legal requirements.

Similarly, the NVE may demand information that is necessary for the implementation of the Regulations relating to Preventive Security and Preparedness in the Energy Supplies, and issue the necessary orders.

Insofar as is necessary for implementing the supervisory functions laid down in or pursuant to the Security Act, the National Security Authority shall be given unhampered access to any area where there is sensitive information or a sensitive object, if the area is owned, used or otherwise controlled by an enterprise.

22 What are the most common enforcement issues and how have regulators and the private sector addressed them?

Limited practice is available and no specific enforcement issues have arisen.

23 What penalties may be imposed for failure to comply with regulations aimed at preventing cybersecurity breaches?

The Norwegian Data Protection Authority may impose a data offence fine of a maximum of 10 times the national insurance basic amount (ie, at present up to 850,000 kroner). Limited practice is available, but we have seen examples that the data offence fines imposed by the Data Protection Authority have been in the range of 500,000 to 700,000 kroner. The Data Protection Authority may also impose coercive fines, which will run for each day from the expiry of the time limit set for compliance with orders issued by the authority until the order has been complied with.

Anyone who wilfully or through gross negligence processed personal data without satisfactory data security may be liable to fines or imprisonment for a term not exceeding one year, or both. In particular aggravating circumstances, a sentence of imprisonment for up to three years may be imposed. Imprisonment is, however, seldom used.

Generally, the supervisory authorities under the different special laws applicable to the private sector (such as the ECA and Regulations relating to Preventive Security and Preparedness in the Energy Supplies) may also impose coercive fines and infringement fines for violations of the relevant laws.

24 What penalties may be imposed for failure to comply with the rules on reporting threats and breaches?

The Norwegian Data Protection Authority may impose a data offence fine (see question 23). The violator may also be liable to fines or imprisonment for a term not exceeding one year, or both, in the case of wilfulness or gross negligence. Other penalties may be available depending on the matter.

25 How can parties seek private redress for unauthorised cyberactivity or failure to adequately protect systems and data?

A party may claim damages from individuals for unauthorised cyberactivities in accordance with general liability rules.

Pursuant to the NPDA, the controller shall compensate damage suffered. The controller may also be ordered to pay such compensation for non-economic damage as seems reasonable.

Threat detection and reporting

26 What policies or procedures must organisations have in place to protect data or information technology systems from cyberthreats?

See question 6.

27 Describe any rules requiring organisations to keep records of cyberthreats or attacks.

Pursuant to the NPDR, any use of the information system that is contrary to established routines, and security breaches, shall be treated as a discrepancy. The purpose of the discrepancy processing shall be to re-establish the normal state of affairs, eliminate the cause of the discrepancy and prevent its recurrence. The discrepancy processing shall be documented in a report containing information on the discrepancy, completed immediate measures, implemented corrective measures, results from evaluating the corrective measures' effect over time, and information on the staff members that have been involved in processing the discrepancy. The reporting is normally done by the staff members that detect the discrepancy, or the staff member who is responsible for handling practices or the affected part of the information system.

Some sectors, such as the financial sector and energy sector, are also obliged to have procedures for recording security breaches that are not necessarily related to personal data. Other rules may be relevant depending on the matter.

28 Describe any rules requiring organisations to report cybersecurity breaches to regulatory authorities.

If a discrepancy has resulted in the unauthorised disclosure of personal data 'where confidentiality is necessary', the Data Protection Authority shall be notified by the data controller (ie, the person or business who determines the purpose of the processing of personal data and which means are to be used). Discrepancies include situations where personal data unintentionally are lost or otherwise have gone missing and unauthorised persons or businesses have accessed, used or procured anyone's personal information. As to the confidentiality requirement, a concrete assessment has to be made to establish whether the disclosed information is confidential.

Providers of electronic communications services are subject to certain reporting requirements to the Norwegian Post and Telecommunications Authority, and organisations within certain sectors, such as the financial sector and energy sector, are also obliged to notify its respective supervisory authorities, in the case of deviations that lead to a material reduction in functionality of the ICT systems or data.

29 What is the timeline for reporting to the authorities?

There is no specific timeline for reporting to the Personal Data Authority, but the reporting shall take place without undue delay from the time the threat of breach became known to the relevant organisation.

Under the Regulations relating to Preventive Security and Preparedness in the Energy Supplies, reporting to the NVE shall be made within three weeks.

30 Describe any rules requiring organisations to report threats or breaches to others in the industry, to customers or to the general public.

It is unclear to what extent the Data Protection Authority may impose an obligation to notify affected individuals or others; however, the authority expects notification following a more concrete assessment of the breach.

The organisation should also consider notifying:

- the police: upon suspicion of theft or other criminal acts;
- insurance companies and other companies: upon contractual obligation to notify;
- special interest organisations: upon standards in the industry requiring notification; and
- credit card companies, financial institutions, credit agencies: if practicalities or damage control require it.

THOMMESSEN

Christopher Sparre-Enger Clausen **csc@thommessen.no**

Haakon VIIs gate 10
0116 Oslo
Norway

Tel: +47 2311 1111
www.thommessen.no

Sweden

Jim Runsten and Ida Häggström
Synch Advokat AB

Legal framework

1 Summarise the main statutes and regulations that promote cybersecurity. Does your jurisdiction have dedicated cybersecurity laws?

In Sweden there are no dedicated cybersecurity laws. The Swedish Civil Contingencies Agency (SCCA, www.msb.se) provides non-binding advice in relation to cybersecurity. Cybersecurity for companies and organisations is often based on the implementation of voluntary measures.

The following relevant provisions can be mentioned.

For governmental authorities the SCCA's Regulation on Governmental Authorities' Information Security applies. Under this Regulation the authorities shall apply a management system for information security including:

- drafting an information security policy;
- appointing persons to coordinate such work;
- classifying its information based on confidentiality, accuracy and availability;
- determining how risk shall be handled; and
- documenting security actions taken.

The management of the authority shall be informed of the work. The work shall be conducted in accordance with ISO 27001:2006 and ISO 27002:2005.

The legislation on security protection involves additional protection for information that is confidential with respect to the nation's safety.

For certain financial companies (see question 8) regulations on information security, IT operations and deposit systems from the Financial Services Authority (FSA) apply in relation to information security.

The Personal Data Act (PDA) contains provisions on processing of personal data. Personal data controllers and processors are required to take certain measures (technical and organisational) to protect the personal data.

The Electronic Communications Act (ECA) applies to electronic communication services and networks. The legislation contains provisions on safety measures required to be taken by providers of electronic communication and service networks (providers) in order to maintain electronic communication and to protect data treated in the systems. Such companies must also report integrity incidents to the controlling authority, the Post and Telecom Authority (PTA).

Certain actions related to cybersecurity are criminalised in Sweden. For example, data breach is a crime according to which it is criminal to give oneself access to data intended for processing by automatic means or unlawfully change, delete or block such data. It is also criminal to interrupt or prevent the use of such data. Such crime entails a fine or imprisonment for a maximum of two years. Data fraud is to give incorrect or incomplete information by amendments to systems, or to unlawfully affect the result of an automatic process that entails gain for the person committing the fraud and damage to someone else. Data fraud entails imprisonment for a maximum of two years. Damages to data systems will be deemed as damage under Swedish criminal statute.

2 Which sectors of the economy are most affected by cybersecurity laws and regulations in your jurisdiction?

All sectors entailing processing of personal data are affected by the provisions on protection for personal data.

Apart from that, the electronic communication services and networks sector and the financial sector are most affected.

Many international standards (such as PCI data security standards and ISO standards) are voluntarily adopted by many companies within the jurisdiction.

3 Has your jurisdiction adopted any international standards related to cybersecurity?

The Swedish Standards Institute (SSI) is a part of the European Committee for Standardization and the International Organization for Standardization. A European standard is always adopted as a Swedish standard. Often ISO standards are adopted as well.

The ISO 27001:2013 has been adopted as a Swedish standard. The entire ISO 27xxx-series has also been adopted by Sweden. The ISO 27037 Digital Evidence is under review and implementation.

4 What are the obligations of responsible personnel and directors to keep informed about the adequacy of the organisation's protection of networks and data, and how may they be held responsible for inadequate cybersecurity?

There are no such obligations for personnel and directors (see question 1). For processing of personal data, a person who is in breach of the PDA can be held responsible and charged with a fine or imprisonment. Such breach may be committed by anyone in breach of the PDA and not only responsible personnel and directors.

5 How does your jurisdiction define cybersecurity and cybercrime?

Under Swedish legislation there are two defined cybercrimes: data breach and data fraud. Both are mainly directed towards registries and systems for automatic processing. In addition, other crimes (not defined as cybercrimes) are often committed through the use of IT technology.

Data breach is to give oneself access to data intended for processing by automatic means or unlawfully change, delete or block such data. It is also criminal to interrupt or prevent the use of such data. Data fraud is to give incorrect or incomplete information by amendments to systems, or unlawfully affect the result of an automatic process that entails gain for the person committing the fraud and damage to someone else.

There is no definition of cybersecurity. The authorities often use the term 'information security'. In the Regulation on Crisis Preparation and Readiness it is stated that: 'information security' entails that 'information systems shall fulfil such basic and specific security requirements to ensure that the authority's business can be conducted in a satisfactory manner. In this context, the need for secure management systems shall be observed.'

For the financial sector 'information security' is defined as 'protection of confidentiality, accuracy and availability'.

Data privacy is related to the protection of people's integrity through use of personal data (all information that can directly or indirectly be related to a living person).

Although there is no general definition of cybersecurity in Sweden, the definition 'data privacy' has a more limited scope only relating to use of personal data whereas cybersecurity and information security relates to security for all types of information.

6 What are the minimum protective measures that organisations must implement to protect data and information technology systems from cyberthreats?

For organisations and companies there are no general requirements regarding protection from cyberthreats.

All organisations and companies that are personal data controllers must adhere to the rules on protection for personal data. The controller of personal data shall, according to the PDA, implement appropriate technical and organisational measures to protect the personal data that is processed. The measures shall provide a level of security that is appropriate with regard to technical possibilities that are available, the cost of implementation, the special risk involved in the processing of personal data and how sensitive the personal data is. The controlling authority for processing of personal data, the Data Inspection Board (DIB) recommends, inter alia, that personal data controllers have a security policy, that the organisation conducts controls in relation to the adherence to the policy and that relevant personnel have education regarding processing of personal data. Further, the DIB recommends that personal data controllers ensure that only authorised personnel have access to the personal data, that access to the data is controlled, that there is a log over use of personal data and that measures are taken to prevent loss of personal data.

Providers of electronic communications and services network adhere to the rules of the ECA. Providers have a confidentiality undertaking regarding subscription information, the content of transferred information (eg, in a text message or telephone call) and other information regarding the communication. Further, providers shall take appropriate technical and organisational measures to protect information treated when providing the services.

A provider adhering to the ECA shall further report to the PTA and any affected users when an integrity incident occurs. An integrity incident is defined as an event leading to involuntary or unlawful deletion, loss or change, or unlawful disclosure or access to information treated in connection to the providing of electronic communication. See question 30 for more details.

See also question 8 for the financial sector.

7 Does your jurisdiction have any laws or regulations that specifically address cyberthreats to intellectual property?

Sweden has adopted the Intellectual Property Rights Enforcement Directive (IPRED), the purpose of which was to improve the protection for intellectual property rights. Under the amendments made in accordance with IPRED a holder of rights can, in the case of an intellectual property right breach over the internet, demand that an internet provider supplies information on, for example, IP numbers of the breaching party. To receive the information, the holder of rights shall issue an application for information injunction in the civil court and must show sufficient evidence of the breach.

8 Does your jurisdiction have any laws or regulations that specifically address cyberthreats to critical infrastructure or specific sectors?

For parts of the financial sector specific rules apply. Banking companies, savings banks, members' banks, credit market companies, credit market associations and investment firms must adhere to the FSA's Regulations and General Guidelines regarding information security, IT operations and deposit systems. According to the Regulations the affected companies shall use a management system to ensure that the information security system work is structured and performed under specific goals set by the board of directors. One person shall be appointed as responsible for leading and coordinating the information security work. Information shall be classified to ensure the right level of protection. The affected companies shall have internal rules for their information security work. The rules shall specify requirements on, for example, physical security, control of access to information and reporting and managing incidents. The affected companies shall ensure that their IT systems are sufficiently secure in relation to the nature of the information processed in the systems. Companies that receive deposits under the rules of the Deposit Guarantee Scheme Act shall have IT systems that ensure access control, system integrity, traceability in the system, etc. The FSA has issued a memorandum on these rules, which may serve as guidance for the application thereof.

To strengthen the control over the financial services sector, there are regulations on how companies that pursue business under the Banking and Financing Business Act may outsource parts of their operations. The company intending to outsource its business must notify the FSA of the outsourcing and provide the FSA a copy of the outsourcing agreement.

For outsourcing, the outsourcing company must at all times remain responsible to its customers for the outsourced activities. The supplier of outsourcing services shall conduct its business with sufficient knowledge, control, and an adequate level of security. Further, the outsourcing cannot have implications on the FSA's ability to monitor the outsourcing company's compliance with its obligations. An outsourcing agreement must be in writing and ensure, among other things, that confidential information is protected.

9 Does your jurisdiction have any cybersecurity laws or regulations that specifically restrict sharing of cyberthreat information?

There are no regulations that specifically regulate cyberthreat information. Therefore, there are no laws or regulations that specifically restrict sharing of cyberthreat information.

10 What are the principal cyberactivities that are criminalised by the law of your jurisdiction?

Data breach and data fraud are cyberactivities that are criminalised. Data breach is when a person gives itself access to data intended for processing by automatic means or unlawfully changes, deletes or blocks such data. It is also criminal to interrupt or prevent the use of such data.

Data fraud is to give incorrect or incomplete information by amendments to systems, or to unlawfully affect the result of an automatic process in a way that entails gain for the person committing the fraud and damage to someone else.

11 How has your jurisdiction addressed information security challenges associated with cloud computing?

When using cloud services for processing of personal data, the personal data controller is always responsible for the personal data. Under Swedish law, the provider of the cloud service will be considered as a data processor. The data controller and the data processor should enter into a written agreement regarding the processing of the data.

The data controller shall always evaluate any possible risks of using a cloud service, for example the technical safety measures taken and in what country the personal data will be stored. The DIB has issued recommendations in relation thereto. The personal data controller should conduct a risk analysis before using a cloud service provider. The greater the integrity risks are for the relevant processing, the greater the requirements for security measures. The integrity risks depend on the number of persons affected by the processing, the amount of data processed for each person and the sensitivity of the data. Measures should be considered for authorisation, authority control, communication security, routines for backup and protection for unauthorised access.

When processing sensitive data (eg, on health), data relating to criminal activities and confidential information, the DIB requires strong authorisation for transfer of data and that the data is protected by encryption. When such data is processed the personal data controller shall also on a regular basis follow up on the identity of the persons who have accessed the data.

12 How do your jurisdiction's cybersecurity laws affect foreign organisations doing business in your jurisdiction? Are the regulatory obligations the same for foreign organisations?

For foreign organisations, the PDA will apply if the organisation is using equipment in Sweden for processing personal data. It should be emphasised that cookies are considered equipment. Therefore, a foreign organisation using cookies on a Swedish website will have an obligation to adhere to the PDA. When the PDA is applicable, the foreign organisation shall appoint a representative who is established in Sweden.

Best practice

13 Do the authorities recommend additional cybersecurity protections beyond what is mandated by law?

As noted above, the legislation on cybersecurity is limited only to use of personal data and for specific sectors. The SCCA provides advice and recommendations regarding information security, which are, however, non-binding.

The DIB also provides advice regarding the processing of personal data. The advice from the DIB will act as the foundation for the DIB's interpretation of the PDA.

14 How does the government incentivise organisations to improve their cybersecurity?

There are no such incentives.

15 Identify and outline the main industry standards and codes of practice promoting cybersecurity. Where can these be accessed?

The ISO 27000 series is used and promoted for management systems. These can be accessed at the SSI's website (www.sis.se). The SSI have also published a manual on information security work, SIS HB 360.

Information on the SCCA's advice can be found at www.msb.se and www.informationssakerhet.se (a website on information security from the SCCA in cooperation with other authorities).

The DIB (www.datainspektionen.se) and the PTA (www.pts.se) also produce advice regarding security for personal data and information regarding electronic communication.

16 Are there generally recommended best practices and procedures for responding to breaches?

No.

17 Describe practices and procedures for voluntary sharing of information about cyberthreats in your jurisdiction. Are there any legal or policy incentives?

The SCCA has taken initiatives to spread information about cybersecurity through the creation of www.informationssakerhet.se, a website containing information and support relating to cybersecurity. The website contains support for management systems for cybersecurity, guidelines and tools, news within the area and facts on the subject.

The PTA generally encourages the public to provide information to the PTA regarding cybersecurity. For example, one of the larger newspapers in Sweden conducted an investigation and a series of articles on the subject of security in the digital community. On the basis thereof, the PTA began an investigation into a large provider of internet and TV services.

18 How do the government and private sector cooperate to develop cybersecurity standards and procedures?

The SCCA has created an information security council with representatives from government and the private sector. The council shall assist the SCCA on information on trends regarding information security, provide opinions on the priority and conduct of the SCCA's work, perform quality certification of the SCCA's work and publicise the SCCA's work.

The PTA hosts an integrity forum for the PTA and representatives from the industry. The forum is held a couple of times each year to discuss issues on integrity in electronic communication. The PTA and DIB also cooperates in matters of information security to exchange information and coordinate its work. The PTA takes part in the international cooperation on integrity issues. The PTA is part of the Contact Network of Spam Authorities and also cooperates with other member states within the European Union on questions for data retention and cookies.

PCI-DSS applies for all entities processing payment data relating to credit or debit cards from distributors to payment transferors and publishers.

19 Is insurance for cybersecurity breaches available in the jurisdiction and is such insurance common?

Certain protection for data breach and damage due to downtime in a system is available through corporate and property insurance.

Enforcement

20 Which regulatory authorities are primarily responsible for enforcing cybersecurity rules?

The DIB is the regulatory authority for the processing of personal data. The PTA is the regulatory authority for the ECA and the processing of data by providers. For the financial institutions mentioned under question 8, the FSA is the regulatory authority.

The SCCA is the regulatory authority for governmental entities' work with information security.

21 Describe the authorities' powers to monitor compliance, conduct investigations and prosecute infringements.

The SCCA coordinates the work regarding the information security, but has no power to monitor compliance.

The PTA supervises the companies providing electronic communication through scheduled supervision activities to investigate whether rules are adhered to. The PTA can also receive knowledge of breaches or irregularities or suspicion of such breach. Based upon such knowledge, the PTA can initiate a supervision activity. The PTA has the right to get access to areas, premises and other spaces where operations to which the legislation applies are conducted. The PTA can place an injunction on an entity, falling under the scope of the legislation, to provide the PTA with information and documents required for control of adherence to the legislation. If the PTA finds that a provider does not adhere the ECA, the PTA my issue injunctions towards such provider to rectify the breach.

The PTA also takes initiatives to promote dialogue with the industry on integrity and other matters. For example, the PTA hosts an integrity forum for the PTA and representative from the industry. The forum is held a couple of times each year to discuss issues on integrity in electronic communication.

The DIB supervises the processing of personal data. The DIB has the right to receive access to the relevant personal data, information on and documentation of the processing of personal data and security for processing. The DIB also has the right to get access to premises connected to the processing of personal data. The DIB may decide on the security measures a personal data controller must take to protect personal data. The DIB may combine such decision with a fine. If the DIB finds that personal data is being processed unlawfully, the DIB shall through dialogue with the personal data controller attempt a correction. If such correction is not possible, or it is urgent, the DIB may prohibit the processing of personal data subject to a fine.

The FSA may request the information and documentation needed for its supervision. The FSA may also visit financial entities to conduct its controls. If a financial entity is in breach of the applicable legislations, the FSA shall issue an injunction to limit or reduce the risks of the business. For material breaches of applicable legislation, the FSA may revoke the permission to conduct financial operations.

22 What are the most common enforcement issues and how have regulators and the private sector addressed them?

The most common issues regarding information security are those related to processing of personal data. For example the DIB has had objections to the content of data processor agreements.

In April 2014 the Data Retention Directive (2006/24/EG) was found invalid by the Court of Justice of the European Communities because the data retention constituted a breach of the right to integrity and privacy. The rules on data retention in the ECA are an implementation of the Data Retention Directive. On the basis of the court's decision, some providers in Sweden ceased their data retention under the ECA. The Swedish government conducted an investigation following the events and found that the ECA was in proportion with the rules on privacy and integrity and that the ECA was valid. However, the providers maintained their opinion on the data retention rules and did not adhere to the data retention rules as set out in the ECA. The PTA has issued injunctions towards the providers to continue data retention according to the ECA. The legal interpretation of the Data Retention Directive and the ECA must be deemed unclear (see 'Update and trends').

23 What penalties may be imposed for failure to comply with regulations aimed at preventing cybersecurity breaches?

If the PTA finds that a provider does not adhere to the ECA, the PTA may issue injunctions towards such provider to rectify the breach. If the breach is not remedied, the PTA may revoke permits to conduct business or issue further injunctions or prohibitions.

If the DIB finds that personal data is being processed unlawfully, the DIB shall through dialogue with the personal data controller attempt a correction. If such correction is not possible, or it is urgent, the DIB may prohibit the processing of personal data subject to a fine. A person committing unlawful processing of personal data, the sanction can be fines or imprisonment of a maximum of six months (or two years if the breach is gross).

Update and trends

New regulation
The EU Data Protection Regulation is still pending implementation, but the goal is to have the regulation adopted during 2015. If the regulation is implemented during 2015 it will come into force by the beginning of 2018. If the regulation is adopted with its current wording it will, for example, give the individual a more defined right to have his or her personal record deleted.

New strategies
The Digital Single Market strategy (DSM) is a strategy developed by the European Commission for online activities. The aim of the DSM is to ensure free movement of services and capital online where individuals and businesses can seamlessly access and exercise online activities under conditions of fair competition, with a high level of consumer and personal data protection, irrespective of the individual's or business's nationality or place of residence. The DSM was adopted on the 6 May 2015 and includes 16 initiatives to be delivered by the end of 2016. Regarding cybersecurity, the third pillar of the DSM regulates trust and security on the web. One part of the third pillar is the European Cybercrime Centre (EC3). The EU has also recognised that trust and security in the digital world are the very foundations of a DSM and one part of that is the Network and Information Security Directive.

Local strategies
During the past years the Swedish government has investigated and chartered the Swedish need for regulations concerning cybersecurity. One of the main findings in the investigation is that there is a need for cybersecurity at most levels in Swedish society. In order to meet the demands for cybersecurity a strategy has been presented to address the lack of cybersecurity in some parts of the public administration.

The purpose of the proposed strategy is to set out fundamental objectives, directions and working methods for cybersecurity in Swedish central government. The strategy has six objectives and areas:
- governance and oversight of cybersecurity in central government;
- central government shall have clear security requirements as a procurer of IT products and services;
- government agencies shall communicate in a secure way;
- government agencies shall report IT incidents to create a basis for improved knowledge and status reports;
- prevention of and fight against cybercrime shall be strengthened; and
- Sweden shall be a strong international partner.

It is not until after the evaluation of any future implementation that a discussion of a civil equivalent can take place. The strategy will, therefore, not regulate any relations between the state and the individual.

Local affects
Within the Swedish Police Department, a new unit against IT crime was established on 1 October 2015. The new national IT crime centre will be the central hub for crimes related to IT and IT crimes and will be in full force by the end of 2017. This unit will be the local Swedish equivalent to the EC3.

If a financial entity is in breach of the applicable legislations, the FSA shall issue an injunction to limit or reduce the risks of the business. For material breaches of applicable legislation, the FSA may revoke the permission to conduct financial operations.

24 What penalties may be imposed for failure to comply with the rules on reporting threats and breaches?

It is only under the ECA that service providers have an obligation to report integrity incidents. Failure to comply with this obligation will entail the sanctions set out in question 23.

25 How can parties seek private redress for unauthorised cyberactivity or failure to adequately protect systems and data?

A party can report personal data breach to the DIB. Regarding electronic communications, a person can report to the PTA, although the PTA has no obligation to address complaints from individuals.

Threat detection and reporting

26 What policies or procedures must organisations have in place to protect data or information technology systems from cyberthreats?

There are no general obligations for organisations to have policies or procedures in place. For governmental authorities, the rules of the SCCA apply. Governmental authorities shall apply a management system including:
- drafting an information security policy;
- appointing persons to coordinate such work;
- classifying its information based on confidentiality, accuracy and availability;
- determining how risk shall be handled; and
- documenting security actions taken.

The management of the authority shall be informed of the work. The work shall be conducted in accordance with ISO 27001:2006 and ISO 27002:2005.

For financial institutions, the rules of the FSA apply. Under these rules the affected institutions must use a management system to ensure that the information security system work is structured and performed under specific goals set by the board of directors. One person shall be appointed as responsible for leading and coordinating the information security work. Information shall be classified to ensure the right level of protection. The affected companies shall have internal rules for its information security work. The rules shall specify requirements on, for example, physical security, control of access to information and reporting and managing incidents. The affected companies shall ensure that their IT systems are sufficiently secure in relation to the nature of the information processed in the systems.

27 Describe any rules requiring organisations to keep records of cyberthreats or attacks.

Integrity incidents shall be reported to the PTA. Providers have an obligation to store certain information for possible use by crime prevention authorities, see question 9.

28 Describe any rules requiring organisations to report cybersecurity breaches to regulatory authorities.

For service providers of electronic communication the ECA applies. Under the ECA, a service provider shall report to the PTA and any affected users when an integrity incident occurs. An integrity incident is defined as an event leading to involuntary or unlawful deletion, loss or change or unlawful disclosure or access to information treated in connection to the providing of electronic communication. See question 30 for more details.

29 What is the timeline for reporting to the authorities?

For integrity incidents, providers with operations under the ECA must report to the PTA within 24 hours of the integrity incident being discovered. The provider must also inform the subscribers or users affected by the incident without undue delay upon discovery of the incident. See question 30.

30 Describe any rules requiring organisations to report threats or breaches to others in the industry, to customers or to the general public.

For providers, the ECA applies. Under the ECA, a provider shall report to the PTA and any affected users when an integrity incident occurs. An integrity incident is defined as an event leading to involuntary or unlawful deletion, loss or change or unlawful disclosure or access to information treated in connection with the providing of electronic communication.

The provider shall, within 24 hours of the incident being discovered, report to the PTA. Information to the PTA shall contain the following:
- when the incident occurred and was discovered;
- the number of affected subscribers or users;
- a description of the incident, its cause and consequences;
- measures to remedy the shortcoming and to avoid similar incidents;
- cooperation with other providers (if the provider is using other providers to provide the service); and
- the effect on subscribers and users in other countries.

The provider must also inform the subscribers or users affected by the incident to enable them to take action to, if possible, mitigate their damage.

A report shall, however, be provided regardless of whether the subscribers or users can mitigate their damage or not. A report to subscribers or users shall be given without undue delay upon discovery of the incident. The information to subscribers or users shall contain the following:

- when the incident occurred;
- a description of the incident and its consequences;
- measures taken by the service provider that have an effect on the subscriber or user;
- recommended measures to be taken by the subscriber or user; and
- contact details to the provider.

The report to the user or subscriber shall be given in a manner that ensures that the information can be received promptly and protected in a suitable manner. The provider shall use its usual method of communication to contact users or subscribers. It is, however, important that the provider takes reasonable actions to ensure that the information reaches the users or subscribers.

synch

Jim Runsten **jim.runsten@synchlaw.se**
Ida Häggström **ida.haggstrom@synchlaw.se**

Birger Jarlsgatan 6
114 34 Stockholm
Sweden

Tel: +46 8 761 35 35
www.synchlaw.se

Switzerland

Michael Isler and Jürg Schneider
Walder Wyss Ltd

Legal framework

1 Summarise the main statutes and regulations that promote cybersecurity. Does your jurisdiction have dedicated cybersecurity laws?

No dedicated cybersecurity legislation has been adopted in Switzerland to date, and there are also no plans to comprehensively address the issue in a bespoke legal instrument. Rather, cybersecurity is and will remain regulated by a patchwork of various acts and regulatory guidance.

In fact, the pertinent legislative landscape has been analysed in a report concerning the national strategy on the protection of Switzerland from cyber risks, which was approved by the federal government in 2012. In a nutshell, the report outlines the existing cybercrime defence scheme and defines the main goals for enhancing protection against cyber risks. After identifying the risks that originate from cyberthreats, the report identifies major weaknesses and resolves how the various stakeholders should proceed. The strategy emphasises three main objectives:

- early identification of threats and dangers;
- improvement of the resilience of critical infrastructure; and
- reduction of cyber risks, especially cybercrime, cyber espionage and sabotage.

The report eventually proclaims 16 measures aimed at minimising cyber risks and enhancing cybersecurity, one of which is dedicated to the validation of the existing legal and regulatory instruments. The report acknowledges that the existing scattered legal framework is inconsistent and incomplete, but also opines that the adoption of a comprehensive cybersecurity regime would be an inappropriate means to address cyber risks. Rather, the existing legislative framework will be subject to continuous adjustment by taking into account the specific exposure to cyber risks within the relevant scope of application of each statute. A corresponding legislative agenda has been devised, but is not publicly accessible.

The following list sets out the most relevant legislative instruments dealing explicitly or implicitly with cybersecurity in the private sector.

Budapest Convention on Cybercrime (CCC)
The CCC entered into force for Switzerland on 1 January 2012. The convention imposes the following main obligations on member states with respect to cybercrime:

- harmonisation of substantive criminal laws;
- adoption of expedient investigation and prosecution measures; and
- setting up a fast and effective regime of international cooperation.

Switzerland's adherence to the CCC brought about some light amendments to the Swiss Penal Code (SPC) and the Federal Act on International Mutual Assistance in Criminal Matters in order to render domestic law compliant with the prerequisites of the convention.

Federal Data Protection Act (FDPA)
The FDPA governs the protection of personal data, which encompasses information pertaining to identified or identifiable natural persons and legal entities. Pursuant to article 7 FDPA, personal data must be protected against unauthorised processing through adequate technical and organisational measures. Enforcement of the data security principles is largely left to self-control by the concerned organisations and, eventually, civil courts; regulatory oversight by the Federal Data Protection and Information Commissioner (FDPIC) in the area of data security, therefore, only exists in isolated cases, but is inexistent on a large scale.

Federal Telecommunications Act (TCA)
Pursuant to article 46 TCA and article 96 of the corresponding Ordinance on Telecommunications Services (OTS), the Federal Office of Communications (OFCOM) is responsible for implementing the administrative and technical requirements pertaining to the security and availability of telecommunications services, which includes notification of the regulator in the event of security incidents. Further, pursuant to article 15 of the Ordinance on Internet Domains, the registry for the '.ch' top level domain (currently the SWITCH foundation) is required, if requested to do so by an OFCOM accredited body to combat cybercrime, to block domain names if there are reasonable grounds to suspect that they are being used to access sensitive data using illegal methods (phishing) or to distribute harmful software (malware). The only organisation entitled to accomplish this task is the Reporting and Analysis Centre for Information Assurance (MELANI).

Federal Act on Financial Market Infrastructure (FinfrAct)
The new FinfrAct, which enters into force on 1 January 2016, regulates the organisation and operation of financial market infrastructures such as stock exchanges, multilateral trade systems, central deposits or payment systems. Article 14 FinfrAct demands robust IT systems that are capable of deploying effective emergency responses and ensure business continuity. The obligations are further detailed in article 15 of the implementing ordinance of the FinfrAct: The systems must be designed in such a way as to:

- ensure availability, confidentiality and integrity of data;
- enable reliable access controls, and
- provide features to detect and remedy security incidents.

Financial market infrastructures are under the regulatory surveillance of the Swiss Financial Market Supervisory Authority (FINMA).

The FinfrAct is the first sector specific federal act applicable to private undertakings that expressly acknowledges the high dependency of essential infrastructure on information technology and the vulnerability to which it is exposed due to the interconnectivity of the market players' systems.

2 Which sectors of the economy are most affected by cybersecurity laws and regulations in your jurisdiction?

The focal zone of regulatory activity in the area of cybersecurity in Switzerland is the financial sector. In the aftermath of the financial crisis, the banking sector suffered from severe data leaks, albeit not primarily due to cyberattacks, which have greatly increased awareness of the importance of data security in general. The FINMA, therefore, amended its circular 2008/21 on the operational risks of banks by adding a new chapter on security of electronic data. Annex 3 to the circular now sets forth a number of principles and guidelines on proper risk management related to the confidentiality of client identifying data stored electronically. The regulator makes clear that state of the art data security standards and procedures as well as proper incident management are pivotal. The main message conveyed is that cybersecurity must become a matter of top management attention.

Another emphasis lies on the protection of critical infrastructure from cyberthreats, such as in the electricity, transportation and

telecommunications sector. The healthcare sector has also received some attention recently, in particular, regarding the vulnerability of medical devices connected to the internet. However, it is fair to state that in small and medium enterprises cybersecurity has not made it to the agenda of many board meetings as an item of strategic importance, but continues being treated as a mere technicality.

3 Has your jurisdiction adopted any international standards related to cybersecurity?

Adherence to international standards related to cybersecurity (such as ISO 27001:2013) is not mandatory in Switzerland. However, many undertakings are undergoing certification voluntarily, and such standards also serve as a benchmark when it comes to compliance with best practices, as, for example, imposed by the regulator in the financial sector or by customers outsourcing their ICT operations to third parties.

Further, pursuant to article 11 FDPA, the manufacturers of data processing systems or programs, as well as private undertakings that process personal data, may submit their systems, procedures and organisations to be evaluated by an accredited independent certification body on a voluntary basis. If they do so (which is very rare), abidance by the standards of ISO 27001:2013 is a prerequisite for such certification.

4 What are the obligations of responsible personnel and directors to keep informed about the adequacy of the organisation's protection of networks and data, and how may they be held responsible for inadequate cybersecurity?

As a matter of principle, the responsibility for cybersecurity lies with the data processing organisation and not with the individuals entrusted with the task. Failure to comply with the data security requirements enshrined in article 7 FDPA does not constitute a criminal offence and, therefore, solely provides civil (tort) remedies to the persons (including legal entities) affected by a breach.

However, the ultimate responsibility for the overall strategy as regards cybersecurity, particularly the determination of the appropriate internal organisation as well as the adoption of the necessary directives, processes and controls, is vested in the board of directors of the company. This is certainly the case with respect to cyber risks that may have an impact on the accuracy of the company's financial statements and, therefore, need to be monitored by an internal control system, which forms part of the statutory audit scope, but may arguably be extended beyond that. Hence, given the increasing importance and awareness of cybersecurity, the problem can no longer be simply delegated to the IT department. In this context, it is notable that, pursuant to article 754 of the Swiss Code of Obligations, the members of the board of directors and other executive directors are personally liable both to the company as well as the individual shareholders and creditors for any loss or damage arising from any intentional or negligent breach of their duties. Hence, personal liability of the responsible individuals might materialise if a company suffered loss because of a severe data breach that is due to lack of appropriate internal cybersecurity controls and procedures.

5 How does your jurisdiction define cybersecurity and cybercrime?

Neither cybersecurity nor cybercrime are defined terms under Swiss statutory laws. There is also no judicial precedence that would help clarify these terms. The neighbouring concept of data security enshrined in data protection legislation has not gained contours either, because it remains vague on the actual degree of security that is necessitated.

The national strategy report on cyber risks adopted by the federal government in 2012 defines cybersecurity as protection from disruptions of and attacks against information and communication infrastructures. Hence, the term would embrace both pertinent operational reliability and extraneous vulnerability concerns.

In line with the scope of application of the CCC, it can be argued that outside heavily regulated sectors cybersecurity in the legislative reality equates defence against cybercrime, namely, repressive sanctions and procedures in relation to the crimes committed through the internet, while preventive security measures are dealt with as a sub-concern of data privacy.

6 What are the minimum protective measures that organisations must implement to protect data and information technology systems from cyberthreats?

Pursuant to article 7 FDPA, personal data (see question 1 for a definition of personal data) must be protected against unauthorised processing through adequate technical and organisational measures commensurate to the type of personal data being processed. Given these vague requirements and even though the FDPA stipulates minimum protective measures, there is a large margin of discretion as to what such minimum requirements would precisely entail (see question 26 for more details).

Even in heavily regulated sectors, such as critical infrastructures, the minimum protective measures are rarely defined. The organisations running the infrastructure are deemed best positioned to assess and implement the actual level of cybersecurity needed for their specific operations and risk exposures. The government would only intervene where self-regulation fails. However, the national cyber risk strategy acknowledges a desire and need to devise more authoritative cybersecurity standards. An interesting observation is that the competitive landscape would not allow the adoption of more stringent (and costly) security requirements on a national level without simultaneous international harmonisation.

7 Does your jurisdiction have any laws or regulations that specifically address cyberthreats to intellectual property?

There is no specific legislation in Switzerland that deals with cyberthreats to intellectual property. Nevertheless, article 39a of the Swiss Federal Copyright Act prohibits the circumvention of effective technological measures for the protection of works and other protected subject matter (digital rights management (DRM)). DRM means technologies and devices such as access control, copy control, encryption, scrambling and other modification mechanisms intended and suitable for preventing or limiting the unauthorised use of intellectual property. It is unlawful to manufacture, import, offer, transfer or otherwise distribute, rent, give for use and advertise or possess for commercial purposes devices, products or components, or provide services that purport the circumvention of DRM.

These prohibitions may not be enforced against persons who are permitted to circumvent DRM by virtue of statutory permission, such as the use of copyrighted work for private purposes or other statutory fair use limitations. It is against this background that the federal government established a surveillance office that monitors and reports on the effects of DRM and acts as a liaison between user and consumer groups. Given its mandate, the surveillance office focuses on the abusive use of DRM systems by the industry rather than on cyberthreats to intellectual property.

8 Does your jurisdiction have any laws or regulations that specifically address cyberthreats to critical infrastructure or specific sectors?

In its 2012 report on cyber risks, the federal government pointed out the fragmented and inconsistent regulation of cybersecurity in critical infrastructure. Although some legislative instruments deal with protection against cyber risks, they generally lack precise definition of the required security measures. The same conclusion was reached by a similar report dealing with the national strategy for the protection of critical infrastructure, which was endorsed by the federal government in the same year.

The primary responsibility to establish suitable controls and procedures lies with the organisations operating critical infrastructure. In the case of the need of governmental intervention, it would, in the majority of cases, be the competent regulator's task to define the appropriate measures. For instance, OFCOM may issue technical and administrative regulations concerning the handling of information security, the obligation to report faults in the operation of networks and other measures that make a contribution to the security and availability of telecommunications infrastructures and services (article 96 paragraph 2 OTS). In the financial sector, it is up to the FINMA to adopt the necessary measures by way of circulars and regulatory notices (article 7 of the Financial Market Supervision Act).

The regulatory activities are seconded by MELANI, which is a body sponsored by the federal government and primarily responsible for counselling a closed circle of roughly 140 operators of critical infrastructure in cybersecurity issues by:

- informing them of cyber incidents and threats;
- providing analyses for early detection and evaluation of cyberattacks and incidents; or
- examining malicious codes.

Given its limited resources, MELANI's activities are limited to the sharing of knowledge and tools that are proprietary to MELANI in its capacity as a governmental agency and cannot be accessed otherwise by the industry, for example, intelligence gathered and pooled by MELANI through the network of the national computer emergency response teams.

9 Does your jurisdiction have any cybersecurity laws or regulations that specifically restrict sharing of cyberthreat information?

Pursuant to the telecommunications secrecy governed by article 43 of the TCA, any person who is or was entrusted with providing tasks pertaining to telecommunications services must not disclose information relating to subscribers' communications or give anyone else the opportunity to do so. The range of addressees of the telecommunications secrecy is very broad and does not only encompass telecom operators, but also all stakeholders that are active in the delivery of telecommunications services, including any auxiliaries entrusted in full or in part with the provision of telecommunications services on behalf of service providers.

The telecommunications secrecy does not only prohibit disclosure of communications content (including peripheral data) to third parties, but also the interception of such content by the addressees of the telecommunications secrecy themselves, subject to the following limitative exemptions:

- lawful interception in accordance with the prerequisites of the Federal Act on the Surveillance of Postal and Telecommunications Traffic;
- filtering of malicious content causing damage to the telecommunications network (viruses, etc) and unsolicited mass advertising; and
- processing of peripheral data for billing and debt collection purposes.

The telecommunications secrecy does not provide for a clear exemption with respect to filtering of malicious content. However, according to article 321-ter paragraph 4 of the SPC, breach of the telecommunications secrecy for the sake of preventing damage is justified and, therefore, not subject to prosecution. On the other hand, pursuant to article 49 TCA, the falsification or suppression of information by a person involved in the provision of telecommunications services constitutes a criminal offence. In a synthesis of these two partially contradicting provisions, the following conditions will apply:

- the filtering must be carried out in an automatic manner to the effect that no individual is capable of taking notice of the content of the information; and
- the objective of the filtering process must be confined to the suppression of the malicious code.

A suppression of the entire message is only permissible if:

- there are no other means of preventing the malicious code from being transmitted; and
- the sender and the intended recipient of the message are informed about the suppression.

10 What are the principal cyberactivities that are criminalised by the law of your jurisdiction?

The following cybercrimes are sanctioned pursuant to the SPC:

- unauthorised obtaining of data (article 143 SPC);
- unauthorised access to a data processing system (article 143-bis SPC);
- damage to data (article 144-bis SPC);
- computer fraud (article 147 SPC);
- breach of secrecy or privacy through the use of an image-carrying device (article 179-quater SPC);
- obtaining personal data without authorisation (article 179novies SPC);
- industrial espionage (article 273 SPC); and
- breach of the postal or telecommunications secrecy (article 321-ter SPC).

Further, the TCA stipulates criminal sanctions where private information received through means of a telecommunication device is used or disclosed to third parties without permission (article 50 TCA), or of the establishment or operation of a telecommunications installation with the intention to disturb telecommunications or broadcasting (article 51 TCA). In addition, processing of data on external devices by means of transmission using telecommunications techniques without informing users thereof is prohibited (article 45c TCA) and constitutes a misdemeanour. Last but not least, transmission of mass advertising through telecommunication channels (spam) constitutes an act of unfair competition and is criminalised as such.

11 How has your jurisdiction addressed information security challenges associated with cloud computing?

Although cloud services have become increasingly popular in Switzerland, there are no specific provisions with regard to the security requirements of cloud computing in Switzerland. Accordingly, the general data protection provisions apply. If personal data are processed in the cloud by a provider, such processing regularly qualifies as data processing by a third party on behalf of the principal as per article 10a FDPA. Pursuant to said provision, the processing of personal data may be outsourced to a cloud provider by agreement or by law if the data are processed only in the manner permitted for the principal itself and the outsourcing is not prohibited by a statutory or contractual duty of confidentiality. Moreover, the principal must ensure that the provider guarantees appropriate data security. Depending on the sensitivity of data processed in the cloud, this may entail an obligation of the principal to conduct security audits, which will often be unrealistic in a cloud setting. In practice, principals will largely rely on the cloud providers' data security certifications, which, however, provide no guarantee that the respective security controls and procedures are actually heeded.

Additionally, cloud computing will frequently entail cross-border disclosure of personal data. According to article 6 FDPA, personal data must not be disclosed abroad if the privacy of the data subjects would be seriously endangered thereby, in particular, due to the absence of legislation in the country of import that guarantees an adequate level of data protection. However, cross-border disclosure through cloud services is generally permissible even in the absence of such comparable privacy legislation, if sufficient alternative safeguards, in particular, contractual clauses, substitute for an adequate level of data protection. Given that in Switzerland data pertaining to legal entities are, in contrast to the majority of European data protection laws, qualified as personal data, outsourcing to the cloud in a cross-border setting almost always triggers the obligation to enter into contractual guarantees.

12 How do your jurisdiction's cybersecurity laws affect foreign organisations doing business in your jurisdiction? Are the regulatory obligations the same for foreign organisations?

There are no specific cybersecurity regulations specifically applicable to foreign organisations doing business in Switzerland. Under Swiss conflict of law rules, a foreign organisation generally needs to observe the provisions of the FDPA if it processes personal data in Switzerland or if data subjects resident in Switzerland are affected, even if the organisation is domiciled abroad. As a general rule, sectorial regulatory requirements pertaining to data security must be heeded by Swiss branches or representations of foreign organisations.

Best practice

13 Do the authorities recommend additional cybersecurity protections beyond what is mandated by law?

MELANI, which is sponsored by the federal government, has adopted recommendations for small and medium enterprises with regard to best practices for removing malware, cleaning up websites, protecting industrial control systems and content management systems, secure e-banking and countering DDoS (distributed denial-of-service) attacks. They are partially based on recommendations issued by the US Industrial Control Systems Cyber Emergency Response Team.

14 How does the government incentivise organisations to improve their cybersecurity?

Apart from the services provided by MELANI, the federal government also has a stake in the public private partnership Swiss Cyber Experts, which is an alliance of cybersecurity experts in the ICT industry, the private and public sector and science. The Swiss Internet Security Alliance is a similar project aiming at reducing the infection rate of devices within Switzerland. Further, cybersecurity projects occasionally receive a grant from the Commission for Technology and Innovation, which is a federal innovation promotion agency responsible for encouraging science-based innovation in Switzerland by providing financing, professional advice and networks. Apart from these examples, no other meaningful incentive schemes exist.

15 Identify and outline the main industry standards and codes of practice promoting cybersecurity. Where can these be accessed?

The pertinent industry norms, such as ISO 27001:2013, can be obtained from the Swiss Association for Standardization against payment (www.snv.ch). Further, MELANI provides some additional guidance (www.melani.admin.ch).

16 Are there generally recommended best practices and procedures for responding to breaches?

Victims of cyberattacks are encouraged to share information and to report incidents to the supporting units maintained by the federal government (see question 17).

17 Describe practices and procedures for voluntary sharing of information about cyberthreats in your jurisdiction. Are there any legal or policy incentives?

Victims of cyberattacks are encouraged to notify incidents to MELANI. The report can be made by a simple message on MELANI's website and may be submitted anonymously. If the victim is also interested in a criminal investigation, a complaint may be filed with the Cybercrime Coordination Unit Switzerland (CYCO). CYCO is Switzerland's reporting channel for illegal subject matter on the internet. Complaint forms are available on its website. CYCO will forward the complaint to the competent prosecution authority in the country.

18 How do the government and private sector cooperate to develop cybersecurity standards and procedures?

The national strategy for the protection of Switzerland against cyber risks, which was adopted by the federal government in 2012, has identified a desire within the industry for intensified cooperation between the public authorities, the private sector and operators of critical infrastructure in order to mitigate cyber risks. Stakeholders expect increased consistency in the elaboration of standards and procedures to be devised in a cooperative manner. The federal government also holds that the primary responsibility to fight cyberattacks lies with each responsible organisational unit individually, and the authorities are only supposed to interfere if public interests are at stake or if the relevant risks cannot be addressed at the competent subordinate level. In line with this strategy, the government is a stakeholder in private initiatives dedicated to the enhancement of cybersecurity awareness and defence schemes (see question 14).

19 Is insurance for cybersecurity breaches available in the jurisdiction and is such insurance common?

At the beginning of 2013, the first insurance company started to offer insurance for cybersecurity in Switzerland. Since then, several Swiss insurance companies have followed this example and offered coverage for cyber risks. The risks insured by those insurances vary significantly and include, for example, the loss or theft of data, unwanted publication of data, damages due to hacking and malware, or costs ensuing from investigations or crisis management as a result of cybercrime.

Enforcement

20 Which regulatory authorities are primarily responsible for enforcing cybersecurity rules?

On a general scale, the following authorities are primarily responsible for enforcing cybersecurity regulations affecting the private sector:

- FDPIC, who is responsible for the supervision of private undertakings with regard to their compliance with the FDPA; and
- CYCO, which forwards cases of incoming reports to the appropriate prosecution authorities in Switzerland and abroad, namely, the police and public prosecutors in charge of prosecuting cybercrimes.

On a sectorial level, the authorities entrusted with regulatory oversight are also responsible for enforcing compliance of the regulated undertakings with cybersecurity rules. In crisis situations affecting critical infrastructure, the special task force for information assurance would intervene. It is composed of decision-makers from the public and private sector dealing with critical infrastructures. Critical infrastructures are those involved in power supply, emergency and rescue services, banks and insurance companies, telecommunications, transport and traffic, public health (including water supply), as well as the government and public administrations.

21 Describe the authorities' powers to monitor compliance, conduct investigations and prosecute infringements.

A distinction must be drawn between the general economy and regulated sectors.

On a general level, the FDPIC is endowed with powers to investigate cases on his or her own initiative or at the request of a third party if methods of data processing are capable of breaching the privacy of a larger number of persons (conceptual systemic failures). This could, for instance, be the case if a specific undertaking processing a large number of sensitive personal data is suspected of neglecting data security obligations. However, the investigative powers would not extend to the examination of data breaches. In the performance of his or her duties, the FDPIC is empowered to request files, obtain information and investigate data processing mechanisms. The FDPIC does, however, not have enforcement powers, but may only issue recommendations. If these recommendations are not complied with, the FDPIC may institute proceedings before the Swiss Federal Administrative court (see question 23 for more details).

In regulated sectors, the authorities do have extended investigative powers within their field of competence. By way of example, the FINMA may appoint independent experts to conduct audits of supervised persons and entities that must provide such experts with all information and documents required to carry out their tasks.

22 What are the most common enforcement issues and how have regulators and the private sector addressed them?

Switzerland has not been exceptionally troubled by cyber incidents in recent years. The most notable event was reported in June 2015, when Iran's nuclear negotiations conducted in Geneva were disturbed by suspicions of cyber espionage in the communication systems of the conference hotel, and the federal prosecutor commenced investigations. On a judicial level, the expectations of expedited international cooperation in combatting cybercrime propagated by the CCC suffered a setback by a landmark decision handed down by the Swiss Federal Supreme Court in January 2015 – the judges ruled that cantonal prosecutors were not empowered to bypass judicial assistance and order Facebook to release the IP history of its users by virtue of article 32 of the convention. With respect to cybersecurity regulations, new rules on the treatment of electronic client data by banks adopted by the FINMA entered into force at the beginning of 2015 and have boosted cybersecurity awareness in the financial sector.

23 What penalties may be imposed for failure to comply with regulations aimed at preventing cybersecurity breaches?

If a recommendation made by the FDPIC in the course of an investigation (referred to in question 21) is not complied with or is rejected by the affected entity, the matter may be referred to the Swiss Federal Administrative Court for a decision. There is also the right to appeal against such decision before the Swiss Federal Supreme Court. However, there are no penalties associated with this.

Failure to comply with rulings of regulatory authorities may constitute a criminal offence or entail administrative sanctions depending on the applicable statute in question.

24 What penalties may be imposed for failure to comply with the rules on reporting threats and breaches?

In the absence of a general obligation to report cyberthreats and data breaches, there are no criminal or administrative penalties associated with such failure. In regulated sectors, failure to submit a required report to the regulatory authority may be prosecuted as a crime or entail administrative sanctions, depending on the applicable statute in question.

25 How can parties seek private redress for unauthorised cyberactivity or failure to adequately protect systems and data?

Victims of cyberattacks may seek redress in a civil action against the tortfeasor. This may be the cybercriminal or the entity that has failed to comply with appropriate data security standards and procedures. Since class actions do not exist in Switzerland, private individuals whose data have been hacked will, in most cases, be incapable of asserting financial damage in an amount that merits a claim.

Threat detection and reporting

26 What policies or procedures must organisations have in place to protect data or information technology systems from cyberthreats?

As mentioned in question 6, personal data must be protected against unauthorised processing through adequate technical and organisational measures. Such measures are set forth in more detail in articles 8 to 12 of the implementing Ordinance to the FDPA. Any systems in which personal data are processed must live up to appropriate state of the art technical standards in terms of protection against risk of unauthorised or accidental destruction or loss, technical flaws, forgery, theft or unlawful access, copying, use, alteration and other kinds of unauthorised processing. More specific requirements are imposed on systems that feature automated processing of personal data. Such systems must, in particular, ensure appropriate access, disclosure, storage and usage controls.

Sector specific regulations do not contain more detailed requirements on the actual standards to be implemented.

27 Describe any rules requiring organisations to keep records of cyberthreats or attacks.

To date, Swiss law does not expressly prescribe such recording obligations.

28 Describe any rules requiring organisations to report cybersecurity breaches to regulatory authorities.

The FDPA does not provide for an explicit obligation to notify data breaches. Should Switzerland ratify the revised Council of Europe Treaty 108 (Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data), a notification obligation in the case of data breaches would have to be included in local law. Pursuant to article 7 paragraph 2 of the revised treaty, the data controller is obliged to notify without delay at least the competent supervisory authority of data breaches that may seriously interfere with the rights and fundamental freedoms of data subjects. Consequently, it is fair to predict that a duty to notify the regulatory authority will be included into the forthcoming amendment of the FDPA.

Sector and critical infrastructure specific notification duties include:

- financial services sector: mandatory notification to the FINMA without delay regarding events of material relevance for the supervision of the relevant supervised entity;
- the telecommunications sector: notification to OFCOM in the case of faults in the operation of telecommunications networks that affect a significant number of customers;
- the aviation sector: notification to the Federal Office of Civil Aviation in the case of safety-related data breaches;
- the railway industry: notification to the Federal Department of the Environment, Transport, Energy and Communications in the case of severe incidents; and
- the nuclear sector: notification to the Swiss Federal Nuclear Safety Inspectorate in the case of safety-related data breaches.

Update and trends

In contrast to its neighbouring countries, Switzerland has no plans to introduce specific IT security legislation, even though the regulatory framework constantly evolves. Especially in critical infrastructures, cybersecurity is becoming a key consideration of the regulatory authorities. By the end of 2017, the measures identified in the federal government's strategy for the protection of Switzerland against cyber risks are supposed to be implemented. It is anticipated that the government's role in cybersecurity will remain a facilitating one, which implies the risk that the synergies created by various private initiatives cannot be leveraged sufficiently. A more resolute pooling of expertise and skills would be desirable.

29 What is the timeline for reporting to the authorities?

The sector-specific provisions mentioned in question 28 require the affected entity to report any relevant cybersecurity incidents without delay.

30 Describe any rules requiring organisations to report threats or breaches to others in the industry, to customers or to the general public.

Scholarly opinion holds that article 4 paragraph 2 FDPA, which stipulates the principle of good faith, entails the rule that data subjects must be informed of unauthorised access to their data. However, such notification duty depends on the gravity of the breach in question. Further, specific contractual obligations may impose on organisations a duty to report threats or breaches.

walderwyss

Michael Isler **michael.isler@walderwyss.com**
Jürg Schneider **juerg.schneider@walderwyss.com**

Seefeldstrasse 123
8034 Zurich
Switzerland

Tel: +41 58 658 58 58
Fax: +41 58 658 59 59
www.walderwyss.com

United Arab Emirates

Stuart Paterson, Benjamin Hopps and Nihar Lovell
Herbert Smith Freehills LLP

Legal framework

1 Summarise the main statutes and regulations that promote cybersecurity. Does your jurisdiction have dedicated cybersecurity laws?

The United Arab Emirates (UAE) consists of seven Emirates, including the Emirates of Abu Dhabi and Dubai. Some Emirates have particular areas within them that have been designated as 'free zones': some free zones have separate civil and commercial laws to those that apply outside the free zone although they remain subject to the UAE federal criminal law.

For the purposes of this chapter, we focus on the laws applying at a federal level in the Emirate of Dubai (including in the Dubai International Financial Centre (DIFC) free zone).

In Dubai, both the federal laws of the UAE and the local Dubai laws will apply. This includes Federal Law No. 5 of 2012 concerning Combating Information Technology Crimes (the Cyber Crimes Law) and Federal Law No. 3 of 1987 concerning the Penal Code (the Penal Code).

The Penal Code contains general provisions prohibiting crimes that will apply to cybercrime, for example those prohibiting the misuse of confidential information. The intention behind the Cyber Crimes Law is to specifically target crimes involving computers, networks and electronic information. It supersedes a number of provisions contained in a number of older federal statutes.

Additionally, government bodies are subject to Cabinet Resolution No. 21 of 2013 concerning Information Security Regulations in the Federal Authorities (the IS Regulations) and Executive Council Resolution No.13 of 2012 regarding the Information Security in the Government of Dubai (the IS Resolution).

In the DIFC free zone DIFC Law No.1 of 2007 (the Data Protection Law) and other associated DIFC laws and regulations will apply in addition to the UAE federal criminal law.

2 Which sectors of the economy are most affected by cybersecurity laws and regulations in your jurisdiction?

The Cyber Crimes Law is intended to apply across all sectors. There are no exceptions.

Anecdotally, cybercrime in the region and in the UAE has targeted a number of sectors. Financial services has been a problem area. There is a significant amount of financial crime in or concerning businesses in the financial sector. Whether the aim is to cripple an institution's systems as a means to extort money, to commit fraud or simply to hack into a system to test its security, an increasing proportion of that crime appears to involve cybercrime as a means to whatever end the cybercriminal seeks to achieve.

In the DIFC, the Dubai Financial Services Authority (DFSA), which regulates banks and other financial providers, suggests that entities follow cybersecurity as a matter of good practice, as well as to meet the DFSA's regulatory requirements.

3 Has your jurisdiction adopted any international standards related to cybersecurity?

The UAE is committed to aligning its cybersecurity laws with international standards. For example, the DFSA strives to ensure that its rules comply with the standards of international organisations including those of the ISO. In its 2014 Annual Report, the DFSA indicated that it would be reviewing its cybersecurity standards against those of ISO 27032 (specifications for improving the state of cybersecurity).

The National Electronic Security Authority (NESA) (responsible for devising cybersecurity for communication and information networks across the UAE and with oversight for protecting the UAE's critical information infrastructure and improving national cybersecurity) has also introduced a framework for tackling cybersecurity issues in a number of papers, including: The National Cyber Security Strategy (NCSS), Critical Information Infrastructure Policy (CIIP) and the UAE Information Assurance (IA) Standards. This framework is a separate standard from recognised international standards but it is understood that it incorporates certain elements of ISO 27001 (specifications for information security management systems).

4 What are the obligations of responsible personnel and directors to keep informed about the adequacy of the organisation's protection of networks and data, and how may they be held responsible for inadequate cybersecurity?

In both the UAE and the DIFC, directors and employees are subject to a duty to act in their organisation's best interests and with reasonable skill and care in the performance of their duties, as provided by Law No. 2 of 2015 concerning Commercial Companies (the UAE Commercial Companies Law). Persons subject to the DIFC's jurisdiction will also have obligations under DIFC Law No. 5 of 2005 (the DIFC Law of Obligations). Entities regulated by the DFSA in the DIFC are also obliged to put in place sufficient operating systems and controls to address risks (including cyberthreats). Should a person fail to uphold his or her duties, he or she can be held liable to pay compensation.

5 How does your jurisdiction define cybersecurity and cybercrime?

None of the Penal Code, Cyber Crimes Law or Data Protection Law contains a definition of 'cybersecurity' or 'cybercrime'.

However, the purpose of the Cyber Crimes Law is to prohibit illegal access to electronic documents or sources or the use of online resources to commit offences, including against the Islamic religion, or to damage the reputation of the UAE.

6 What are the minimum protective measures that organisations must implement to protect data and information technology systems from cyberthreats?

The UAE currently has no federal legislation imposing obligations on organisations relating specifically to cybersecurity in relation to data protection. It is anticipated that such a law will be developed in the future. However, there is various sector-specific federal legislation in place which prohibits the disclosure of sensitive and confidential data; for example, Federal Law No. 6 of 2010 (the Credit Information Law) requires commercial banks and financial institutions in the UAE to provide the Credit Bureau with data on credit information: such information must be kept confidential and the data subject's consent must be sought before any proposed disclosure of his or her information. Moreover, under the Penal Code, it is a criminal offence to disclose confidential information without the requisite consent.

Organisations operating in the DIFC will be subject to the requirements of the Data Protection Law and associated regulations. For example, transfers of personal data outside of the DIFC may only occur if the receiving jurisdiction has an adequate level of protection in place. Additionally, an individual subject to the Data Protection Law must implement appropriate technical and organisational measures to protect personal data from unauthorised disclosure, wilful or accidental loss and other unlawful use of the personal data.

7 Does your jurisdiction have any laws or regulations that specifically address cyberthreats to intellectual property?

Not specifically. In the UAE, intellectual property rights are protected through various pieces of federal legislation such as:

- Federal Law No. 17 of 2002 (as amended by Federal Law No. 31 of 2006) regulating and Protecting the Industrial Property of Patents, Industrial Drawings and Prototypes (the Industrial Property Law);
- Federal Law No. 7 of 2002 in respect of Author Copyright and Parallel Rights (the Copyright Law); and
- Federal Law No. 37 of 1992 (as amended by Law No. 19 of 2000 and Law No. 8 of 2002) concerning Trade Marks (the Trade Marks Law).

The DIFC does not currently have a separate regime for the protection of intellectual property rights. In 2009, however, the DIFC issued draft intellectual property laws for public consultation. It is expected that these may be formally implemented in the future.

Any breaches of these intellectual property rights in the Emirate of Dubai can be pursued as a civil or criminal claim under the Penal Code and Civil Code. However, none reference cyberthreats directly.

8 Does your jurisdiction have any laws or regulations that specifically address cyberthreats to critical infrastructure or specific sectors?

No.

9 Does your jurisdiction have any cybersecurity laws or regulations that specifically restrict sharing of cyberthreat information?

Yes. Federal Law No. 3 of 2003 regarding the organisation of the telecommunications sector (the Telecoms Law) criminalises illegal access or obstructions to telecommunications services as well as the interception of private communications without the requisite permission from the judicial authorities. There are no specific laws or regulations that specifically restrict sharing of cyberthreat information in the UAE.

10 What are the principal cyberactivities that are criminalised by the law of your jurisdiction?

UAE legislation is aimed at combating criminal activity on the internet and on any other electronic sources as well as the protection of confidential and sensitive information. For example, it is an offence to:

- obtain unauthorised access to electronic sources;
- forge an electronic document;
- disclose confidential electronic documents without permission;
- slander a third party online;
- make online offensive comments against the Islamic religion; or
- publish online information that damages the reputation of the UAE and its rulers.

11 How has your jurisdiction addressed information security challenges associated with cloud computing?

The UAE does not have a specific legislative framework which addresses the risks associated with cloud computing services. Federal Law No. 2 of 2006, for example, would cover the criminal actions of a hacker who accessed data held in a cloud computing environment but would not address the liability of the cloud provider to its injured user. Outside the DIFC, there is no single law in the UAE that deals with data protection or information security.

General laws – outside the scope of any contractual rights expressly conferred by a cloud provider – provide a limited amount of protection for users of cloud services. A cloud user who suffers loss as a result of an outage or a security breach on the part of the cloud provider could make a claim for compensation under the Civil Code; however, it would have to prove the value of that loss to establish its claim, which may be difficult.

12 How do your jurisdiction's cybersecurity laws affect foreign organisations doing business in your jurisdiction? Are the regulatory obligations the same for foreign organisations?

Yes, foreign organisations doing business in the UAE will be subject to the UAE's cybersecurity laws. The UAE's cybersecurity laws do not distinguish between local and foreign organisations.

It may be particularly difficult to bring a claim against a cloud provider that is based overseas, especially as there is no specific law or regulation in the UAE that addresses potential claims arising from the cloud computing relationship. Where data is transferred across different jurisdictions, it will be necessary to determine which laws would apply in the event of a security breach.

Federal Law No. 18 of 1993 (the Commercial Transactions Law) imposes data retention obligations on UAE companies. A company based in the UAE (including the DIFC) should take care to ensure that it can comply with these data retention obligations at all times, including where there is a failure by the cloud provider, particularly if that cloud provider is based overseas and is not subject to the same obligations.

Best practice

13 Do the authorities recommend additional cybersecurity protections beyond what is mandated by law?

The UAE authorities are committed to tackling cybercrime in order to minimise any threats to the stability of the UAE. The Ministry of Justice and other international government bodies share ideas on countermeasures to defend their countries from cybercrime. The UAE authorities have conducted awareness campaigns to highlight cybersecurity threats and suggested voluntary preventive measures to be adopted. For example, both the police and the telecoms regulatory authority ran a cyber blackmail awareness campaign in 2015 to educate the general public on the risks and consequences associated with the sharing of data.

14 How does the government incentivise organisations to improve their cybersecurity?

As there is limited taxation in the UAE, such an incentive is not available to the authorities here to the extent that it is elsewhere. Instead, the UAE authorities are keen to emphasise the benefits of a safe cyber-technology infrastructure, pointing to regional and international cooperation, and cooperation between the UAE government and private sector, as essential elements of achieving successful cybersecurity.

15 Identify and outline the main industry standards and codes of practice promoting cybersecurity. Where can these be accessed?

There is no set industry standard or code of practice on cybersecurity in the UAE. However, many organisations are encouraged to adopt ISO standards where possible and to voluntarily develop and review internal policies as a matter of good practice. In addition, and drawing on a number of standards and guidance such as ISO 27001, NESA has produced a set of standards and guidance for government entities in certain critical sectors. Compliance with these standards is mandatory.

16 Are there generally recommended best practices and procedures for responding to breaches?

There are no UAE-specific or government-endorsed best practices. However, a sensible starting point for an organisation would be to establish a committee or department responsible for the oversight of cybersecurity, to be responsible for regularly reviewing and implementing the organisation's business processes and assessing the risks involved with these.

Internal policies should be developed for encouraging cybersecurity. Regular reporting and monitoring of cybersecurity breaches should be encouraged. Clear and established reporting lines and response measures are important.

Organisations should also develop a practice for educating and training employees on cybersecurity risks and consequences. HR policies on the vetting of employees would also minimise any potential risks posed by an organisation's employees.

Post-breach response strategies should be implemented. These should include guidelines for the organisation's interactions with the media, customers and regulatory or enforcement authorities, and the retention of third-party forensic firms to assist with any investigations that may result from a breach.

17 Describe practices and procedures for voluntary sharing of information about cyberthreats in your jurisdiction. Are there any legal or policy incentives?

There is no set guidance or procedure in the UAE as to the voluntary sharing of information about cyberthreats. However, the UAE authorities have in the past issued press releases through local newspapers encouraging organisations to share information about cybercrimes and potential foreseeable cyberthreats. Additionally, the fact that a failure to report a crime in the UAE could attract severe criminal penalties under the Penal Code acts as an incentive for organisations to share information on cyberthreats.

18 How do the government and private sector cooperate to develop cybersecurity standards and procedures?

Cooperation between the government and the private sector occurs through:

- consultation papers on proposed legislation;
- joint training seminars and case studies; and
- voluntary sharing of information on suspected or imminent cybersecurity breaches.

19 Is insurance for cybersecurity breaches available in the jurisdiction and is such insurance common?

Yes. It is increasingly common.

Enforcement

20 Which regulatory authorities are primarily responsible for enforcing cybersecurity rules?

NESA is the principal regulatory authority in the UAE which oversees compliance with cybersecurity rules and cybercrime prevention across the Emirates.

The Dubai Electronic Security Centre (DESC) is tasked with the protection of the Dubai government's information and telecommunications network and information systems.

The Commissioner of Data Protection (the Commissioner) is responsible for monitoring and enforcing data protection laws in the DIFC. A person wishing to undertake sensitive data processing in the DIFC or to transfer such data out of the DIFC will be required to make an application to the Commissioner for a permit to do so.

The Dubai police have a dedicated cybercrimes department. Where any criminal offences are suspected, the police will necessarily be involved in the investigation and prosecution of such offences.

21 Describe the authorities' powers to monitor compliance, conduct investigations and prosecute infringements.

As part of their investigation or prosecution, the police have the power to enter private premises to conduct searches and seize documents. Additionally, the police can interview witnesses and the accused in the course of their collection of evidence.

In addition, NESA and DESC have power to take any necessary measures to prevent cybercrime incidents. For example, they may control access to any communication or information networks.

The Commissioner's function is to uphold good practices in data protection and encourage adherence to the requirements of the Data Protection Law in the DIFC. The Commissioner has the power to do whatever he or she deems necessary for or in connection with his or her function. This may include issuing document or information requests and requests for interviews.

22 What are the most common enforcement issues and how have regulators and the private sector addressed them?

Criminal prosecutions are often not publicly reported in the UAE and examples of enforcement actions are rare. Figures released by Dubai police's cybercrimes department show that it received 1,549 reports in 2014, broken down as follows: 248 fraud cases, 163 information security cases, 389 extortion and libel cases, 235 website crimes and 514 miscellaneous cybercrimes.

However, banks and financial services companies in Dubai and the DIFC are particularly susceptible to cyberattacks. The DFSA, as part of its risk supervision strategy, urges DIFC companies to ensure that due attention and importance is given to cybersecurity measures, particularly any controls they may have over a third-party provider.

23 What penalties may be imposed for failure to comply with regulations aimed at preventing cybersecurity breaches?

Any breach of the Cyber Crimes Law will be a criminal offence and offenders will be prosecuted by the relevant UAE authority in conjunction with the police. A conviction may result in fines, imprisonment or deportation. The UAE authorities also have the power to confiscate any devices, programs or other means used in the commission of criminal offences or to destroy them, as well as the ability to close the place of crime indefinitely or for a period specified by the court.

Breaches of the Data Protection Law and associated regulations by a person subject to the DIFC's jurisdiction will be a civil matter and investigated by the Commissioner. Following an investigation, the Commissioner has the discretion to issue a direction to require a person to either undertake to do or to refrain from doing a particular act relating to the personal data, impose fines, make a person liable for the payment of compensation or initiate court proceedings.

24 What penalties may be imposed for failure to comply with the rules on reporting threats and breaches?

Company officers in both Dubai and the DIFC will be subject to an overriding fiduciary duty to act in the best interest of their shareholders and other stakeholders (see question 4) and will be liable to pay compensation if a breach of duty can be established.

In addition, there is also a general obligation under the Penal Code to report a crime and to refrain from giving false information. A failure to comply with this obligation can lead to a fine.

25 How can parties seek private redress for unauthorised cyberactivity or failure to adequately protect systems and data?

In Dubai, private redress may be possible by way of a civil claim under the Civil Code and the Commercial Companies Law where it can be established that a person is responsible for or has negligently contributed to the harm done to the aggrieved party. There is therefore a risk that, if a person is found to be negligent in the reporting of cybersecurity threats and breaches, they will be liable to pay compensation to the wronged party.

In the DIFC, a person who is a data subject (defined as an individual to whom the personal data relates; this definition can extend to persons who are employees or customers of the relevant DIFC entity that receives their data), and who believes on reasonable grounds that they have been adversely affected by a data controller's breaches of the Data Protection Law and associated DIFC regulations, may lodge a complaint with the Commissioner. The Commissioner may then mediate between the data subject and the data controller. Following the mediation, the Commissioner may issue a direction requiring the data controller to do what it considers appropriate, which can include the suspension of any data processing for a certain period of time or indefinitely.

Additionally, a person who suffers damage for any reason through the failure of the data controller to adhere to the Data Protection Law and associated DIFC regulations may make an application to the DIFC Court for compensation.

Threat detection and reporting

26 What policies or procedures must organisations have in place to protect data or information technology systems from cyberthreats?

The DFSA suggests that DIFC companies should aim to proactively implement cybersecurity measures that meet the highest international standards. As a guideline, DIFC-based branches of UK entities should look to comply with the expected standards of the Financial Conduct Authority (FCA) which, following its recent thematic reviews into financial crime, offers practical guidance to entities seeking to improve their cybersecurity

standards. Although there is no obligation to use it as such, this guidance would also provide a good model for entities that are not connected to the UK but which are looking for a sensible starting point. The FCA, for example, considers it good practice:

- for a senior manager to be appointed and tasked with the overall responsibility for data security and liaising with stakeholders within the entity;
- for an entity to seek external assistance if there is insufficient expertise within the firm to carry out a risk assessment of data security policies and procedures;
- to encourage the regular testing of staff understanding of data security and why it is important to their work;
- to set up formal vetting procures for the employment of staff with access to sensitive data;
- to require the use of robust passwords;
- to use tailored IT software designed to spot suspicious activity;
- to encrypt data, particularly that which is on back-up tapes in storage or which is being transported; and
- to block access to all internet-based content which allows web-based communications.

27 Describe any rules requiring organisations to keep records of cyberthreats or attacks.

Although there are no specific UAE laws requiring organisations to keep records of cyberthreats or attacks, organisations are required to keep records of trading activities for at least five years.

In the DIFC, organisations are required under the Data Protection Law and associated regulations to keep records of any data processing operations and to notify the Commissioner where there are any discrepancies in the data processing.

28 Describe any rules requiring organisations to report cybersecurity breaches to regulatory authorities.

See question 24. In order to make a report to the police, a written summary (in Arabic) of the background and the offence, together with supporting documents must be lodged at a police station.

Update and trends

The relatively recent introduction of the Cyber Crimes Law highlights the UAE's commitment to preventing and minimising cybercrime. The Cyber Crimes Law has a broad application across all sectors and is intended to supplement any sector-specific legislation. The UAE police have been keen to monitor cybercrime since its implementation.

Given that technology is in a constant state of flux, and the tendency of criminals to develop new ways to commit crimes, cybersecurity is understandably a permanent fixture on the agendas of the UAE government and many organisations. The principal challenge to the development of cybersecurity regulations at government level is the typically long lead time for new laws to become enacted, and the inevitable lag between this and criminals' new methods. Organisations, on the other hand, will need to ensure that they have adequate resources (human and financial) to devote to the continued implementation and review of good cybersecurity standards and to take proactive steps in reducing cybercrime incidents.

29 What is the timeline for reporting to the authorities?

There is no specific time period. The authorities should be notified as soon as possible as soon as a person or organisation becomes aware of a serious cybersecurity threat or breach. A delay in doing so may attract civil and criminal penalties, as mentioned in question 24.

Organisations should establish adequate monitoring and reporting policies to encourage a culture of reporting internally.

30 Describe any rules requiring organisations to report threats or breaches to others in the industry, to customers or to the general public.

There are no specific UAE laws on the reporting of threats or breaches by organisations to persons other than the authorities. However, as a matter of good practice, an organisation should aim to establish reporting protocols to undertake in the event of a cyberthreat or breach in order to manage risks.

HERBERT SMITH FREEHILLS

Stuart Paterson **stuart.paterson@hsf.com**
Benjamin Hopps **benjamin.hopps@hsf.com**
Nihar Lovell **nihar.lovell@hsf.com**

Dubai International Financial Centre
Gate Village 7, Level 4
PO Box 506631
Dubai
United Arab Emirates

Tel: +971 4 428 6300
Fax: +971 4 365 3171
www.herbertsmithfreehills.com

United States

Benjamin A Powell, Jason C Chipman and Leah Schloss
Wilmer Cutler Pickering Hale and Dorr LLP

Legal framework

1 Summarise the main statutes and regulations that promote cybersecurity. Does your jurisdiction have dedicated cybersecurity laws?

The United States generally addresses cybersecurity through sector-specific statutes, regulations and private industry requirements.

At the federal level, numerous agencies impose cybersecurity standards through a variety of regulatory and enforcement mechanisms. For example, the Federal Information Security Management Act of 2002 (and implementing guidance) establishes cybersecurity standards for federal government agencies and their contractors. Similarly, the Gramm-Leach-Bliley Act (GLBA) and the Health Insurance Portability and Accountability Act (HIPAA) (and implementing regulations and agency guidance) require entities in the financial services and health sectors, respectively, to employ technical, administrative and physical safeguards to protect customer information from unauthorised access or use. Several states have also enacted state parallels to the GLBA and HIPAA requirement. The Federal Risk and Authorization Management Program (FedRAMP) is a government-wide programme that provides a standardised approach to security assessments, authorisation and continuous monitoring for companies providing cloud services to federal civilian agencies.

In 2015, the Department of Defense (DoD) enacted a potentially significant interim rule (meaning that the rule is in effect but may be further refined when finalised) applicable to companies that do business with the US defence community. The new rule is a DoD regulation that establishes prescriptive cybersecurity requirements as part of the Defense Federal Acquisition Regulations Systems (DFARS), which mandates the use of cybersecurity-related contract clauses in all DoD contracts. These clauses are mandatory 'flowdown' terms to subcontractors at all tiers. The rule, which includes requirements with respect to security controls and cyber incident reporting, has been highly criticised by industry as being overly burdensome and in need of revision. The rule is currently in effect, but it was open to a public comment period, and may be changed through the standard regulatory process. In fact, DoD has already announced its intent to issue a new interim rule.

For companies handling consumer data, the Federal Trade Commission (FTC), the main federal consumer protection agency responsible for enforcing the prohibition on 'unfair and deceptive acts or practices,' frequently enforces minimum security requirements with respect to entities collecting, maintaining or storing personal information. In June 2015, the FTC issued 'Start with Security' guidance, which identifies the FTC's lessons learned from 50+ data security enforcement actions brought by the FTC since 2001. This guidance advises companies to incorporate a series of 10 lessons learned, ranging from authentication controls to network segmentations.

For publicly-traded companies, the Sarbanes-Oxley Act of 2002 (SOX) and implementing regulations require publicly-traded companies to maintain a system of internal controls over financial reporting. Regulatory guidance has stated that '[m]anagement's evaluation of the risk of misstatement [of financial reports] should include consideration of the vulnerability of the entity to fraudulent activity [...] and whether any such exposure could result in a material misstatement of the financial statements'. To meet these requirements, companies are audited to determine the extent to which they maintain a series of IT 'general controls' (ITGC) on systems designated as related to financial reporting.

Some subject-matter specific cybersecurity standards focus narrowly on a single constituency or a single government agency. For example, the Veterans Affairs Information Security Enhancement Act, passed in 2006 as part of the Veterans Benefits, Health Care, and Information Technology Act, requires the Department of Veterans Affairs (VA) to implement agency-wide information security procedures to protect sensitive personal information held by the VA and VA information systems. There are also numerous pending legislative proposals to regulate the security of certain sectors, including the automotive sector, data brokers and certain energy companies.

A handful of states have also adopted general security requirements that apply to companies conducting business in their state, collecting personal information about residents or citizens of their states, or both. A primary example is the Massachusetts Standards for the Protection of Personal Information of Residents of the Commonwealth. These regulations require companies collecting personal information about Massachusetts residents to develop written information security programmes containing administrative, technical and physical safeguards. Other states have enacted narrower requirements such as security requirements for particularly sensitive information (eg, payment card data, mental health information, etc) and secure disposal requirements for electronic or paper media containing sensitive personal information.

In the criminal context, the Computer Fraud and Abuse Act (CFAA) 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 (ECPA) 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 (SCA) 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.

Beyond regulatory standards, many organisations are subject to voluntary standards or are required by contract to comply with cybersecurity requirements. Of particular note, the payment card industry in the United States establishes its own cybersecurity standards (the Payment Card Industry Data Security Standards (PCI-DSS)) that apply to merchants or vendors that process payment card data. The federal government has also focused substantially in recent years on the establishment of voluntary cybersecurity requirements, particularly for critical infrastructure entities, which are generally entities that provide vital services to a large part of the population. In 2013, the President issued Executive Order 13636, 'Improving Critical Infrastructure Cybersecurity' to establish a process for the government to create voluntary cybersecurity standards applicable to critical infrastructure entities. Pursuant to this Executive Order, the National Institute of Standards and Technology (NIST) issued a voluntary 'Cybersecurity Framework', which provides a risk-based approach to cybersecurity, and references various national and international standards.

2 Which sectors of the economy are most affected by cybersecurity laws and regulations in your jurisdiction?

In several respects, the financial services industry and the health-care sector are the most regulated sectors with regard to cybersecurity. Federal banking agencies promulgated several data security guidelines in 2000, including the 'Interagency Guidelines Establishing Information Security Standards'. This guidance states that certain covered 'financial institutions' are required to implement comprehensive written information security programmes including administrative, technical and physical safeguards 'appropriate to the size and complexity' of the financial institutions and 'the nature and scope of its activities'. The financial regulators, through the Federal Financial Institutions Examination Council (FFIEC), have also issued a series of booklets as part of the IT Examination Handbook, covering issues ranging from information security to outsourcing technology services to management and governance. The Securities and Exchange Commission (SEC) has also issued guidance to public companies (as well as to the financial services institutions it regulates), and has articulated steps the SEC will take in the future to ensure cybersecurity preparedness in the securities sector. In the health-care sector, under HIPAA, the Department of Health and Human Services (HHS) has adopted security standards to protect individually identifiable health information.

3 Has your jurisdiction adopted any international standards related to cybersecurity?

The United States has not adopted any international cybersecurity standards into law. However, NIST has created a 'Cybersecurity Framework,' pursuant to Executive Order 13636, establishing voluntary standards applicable to critical infrastructure companies that incorporate many of these international benchmarks as examples of best practice to help US companies manage and reduce cybersecurity risks.

4 What are the obligations of responsible personnel and directors to keep informed about the adequacy of the organisation's protection of networks and data, and how may they be held responsible for inadequate cybersecurity?

All directors and officers (D&O) owe their companies the fiduciary duties of care, loyalty and good faith. Given the broad-based impact of cybersecurity threats and data breaches on business viability and reputation, D&Os can no longer expect their company's IT department to successfully manage these concerns in isolation. Instead, successful boards lead their organisations in addressing and incorporating cybersecurity concerns into all facets of business decision-making and processes.

Regulators, particularly in the financial services sector, have made clear that they expect board and management involvement in data security. For example, the financial sector Interagency Guidelines Establishing Information Security Standards provide that the board of directors or an appropriate committee of the board shall approve the entity's written information security programme and oversee the development, implementation and maintenance of the programme, including assigning specific responsibility for its implementation and reviewing reports from management. Similarly, the FFIEC issued an updated version of the Management Booklet of its IT Examination Handbook in November 2015, which emphasizes the importance of board oversight and management implementation of effective IT programmes, including IT security.

US corporate directors are, generally, not required by law to have specific expertise in cybersecurity areas. D&Os are generally responsible for proactively monitoring, managing and educating themselves on risks to the company, including cybersecurity risks and trends. Boards that fail to account for cybersecurity risks to a business may leave their companies vulnerable to a variety of civil litigation claims for failure to adequately maintain cyber and data protections, and prevent unauthorised access to consumer personal and financial information. In light of the growing emphasis on managing cybersecurity concerns, an increasing number of companies in the United States hire outside experts to report to the board on cybersecurity issues on a regular basis. In addition, boards are increasingly examining board committees to ensure that there is appropriate board oversight of the company's data security and privacy procedures.

5 How does your jurisdiction define cybersecurity and cybercrime?

The United States lacks consistent and clear definitions for cybersecurity and cybercrime. In general, cybercrime is defined by the CFAA as accessing a protected computer without authorisation or exceeding authorised access to such protected computer. A 'protected computer' includes computers used in interstate communication, such as computers connected to the internet. 'Cybersecurity' is generally not defined in law, although DoD and the General Services Administration published recommendations in 2014 calling for common cybersecurity definitions for federal acquisitions in order to increase efficiency and effectiveness in the public and private sector.

6 What are the minimum protective measures that organisations must implement to protect data and information technology systems from cyberthreats?

Industries vary with respect to the protective measures required to be taken to thwart cyberthreats and data breaches. Both health-care and certain financial services entities have minimum requirements they are required to meet. However, these requirements are generally broad and do not include specific technical standards. For example, although HHS regulations identify a specific level of encryption that companies should use, companies are not required to use it. Instead, encrypting data provides a safe harbour for companies otherwise facing notice obligations in the event of a data security breach. Under the new DoD-mandated contract clauses, DoD contractors and subcontractors holding certain (broadly defined) categories of information (covered defence information) are required to comply with security requirements prescribed in NIST Special Publication 800-171, 'Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations,' while DoD contractors and subcontractors providing IT services or cloud services are required to comply with other security requirements specified in the contract or in DoD cloud security guidance. Contractors providing cloud services to civilian government agencies under FedRAMP are also required to comply with certain contractual security requirements.

Merchants, payment processors and other parties dealing in payment cards, such as credit cards, are required to comply with various technical requirements under PCI-DSS, which are implemented via contract between parties and are not enacted into law. These standards include 12 categories of requirements that companies must meet with respect to the security of payment card information. Companies failing to comply risk fines from the payment card brands.

Apart from these mandatory standards, NIST's Cybersecurity Framework created in response to Executive Order 13636 catalogues best practices for identifying, protecting, detecting, responding to and recovering from cybersecurity incidents by creating adaptable benchmarks and recommendations. While these standards are explicitly not mandatory, some have suggested that widespread adoption of this Framework by companies may result in the Framework representing a new 'standard of care' for US businesses generally.

7 Does your jurisdiction have any laws or regulations that specifically address cyberthreats to intellectual property?

Both the Digital Millennium Copyright Act and the CFAA prohibit certain cyberthreats to US intellectual property rights, including threats arising from cyber intrusions.

In addition, the federal government has issued two strategies under President Obama to address cyberthreats to US trade secrets and intellectual property rights. The 'Strategy on Mitigating Theft of US Trade Secrets' aims to protect US trade secrets abroad, promote voluntary best practices, enhance domestic law enforcement and improve legislation. The 'Joint Strategic Plan on Intellectual Enforcement' focuses on improving transparency in intellectual property policy and rulemaking, ensuring interagency coordination and securing US rights abroad.

Several pieces of pending legislation seek to protect US intellectual property rights and trade secrets from foreign governments and allegedly government-sponsored entities involved in hacking US computers and networks.

8 Does your jurisdiction have any laws or regulations that specifically address cyberthreats to critical infrastructure or specific sectors?

Some federal agencies in the United States have promulgated standards associated with protecting critical infrastructure entities from cyber intrusions. Of particular note, the Federal Energy Regulatory Commission (FERC) has established 'Critical Infrastructure Protection Reliability Standards' to address potential vulnerabilities in the bulk-electric system.

These standards require certain electricity grid 'bulk-power' system asset owners and operators to document, report and provide compliance evidence on a variety of security controls to the North American Electric Reliability Corporation (NERC) and FERC. They also require the characterisation of all cyber systems that influence the bulk-electric system as low, medium or high impact. In addition, these standards call for responsible entities to identify, assess and correct deficiencies in their cyber policies. Additionally, the Transportation Security Administration (TSA) has statutory authority to promulgate regulations related to pipeline physical security and cybersecurity, though it has not yet exercised this authority to issue cybersecurity requirements. And, as discussed above, the financial, health care and government contracting sectors are subject to regulatory or contractual requirements to implement administrative, technical and physical safeguards to prevent or mitigate a cyberattack.

The President of the United States has also issued Executive Order 13636, 'Improving Critical Infrastructure Cybersecurity', that calls for the enhancement of security measures to protect critical infrastructure. This Executive Order does not establish mandatory standards but, instead, requires the creation of minimum voluntary standards for the protection of critical infrastructure entities. In so doing, it attempts to balance efficiency, safety, privacy, business confidentiality and civil liberties in the cybersecurity realm. Pursuant to this Executive Order, NIST issued a voluntary 'Cybersecurity Framework', which provides a risk-based framework and identifies best practices for identifying, protecting, detecting, responding to and recovering from cybersecurity incidents. The Cybersecurity Act of 2015, which was enacted in December 2015, includes several significant provisions designed to facilitate the sharing of cybersecurity threat data among the government and private sector companies, and marks the end of a multi-year effort to find a compromise between industry demands for liability protection for cybersecurity information-sharing and privacy concerns regarding government access to such information.

9 Does your jurisdiction have any cybersecurity laws or regulations that specifically restrict sharing of cyberthreat information?

In the United States, ECPA, which includes the SCA, restricts sharing of, and government access to, certain private electronic communications. ECPA includes three titles. Title I outlaws unlawful interceptions of wire, oral and electronic communications. Title II is the SCA, which restricts the disclosure of electronic communications held in electronic storage by third-party electronic communication and remote computing service providers. Title III regulates the use of pen registers or trap and trace devices, which are devices that can acquire metadata, such as phone numbers. Many states have similar laws against government and private wiretapping, some of which are even more stringent than the federal laws, including some states with two-party consent requirements for wiretapping.

The GLBA Privacy Requirements mandate that financial institutions give consumers privacy notices that explain the institution's information-sharing practices. Consumers also have the right to opt-out and limit some of the information shared. Financial institutions must protect the information collected about individuals, except for information collected in business or commercial activities. Other statutes, such as the Right to Financial Privacy Act, restrict the sharing of certain financial information with the government, subject to several exceptions.

In the health-care sector, the HIPAA Privacy Rule protects all individually identifiable health information stored or transmitted by a covered entity or its business associate in any media. In particular, the HIPAA Privacy Rule regulates how covered entities use and disclose protected health information. It also creates limitations on the release of health records to third-parties, creates accountability through civil and criminal penalties and enables patients to determine how their information is used and whether any disclosures have been made.

The Cybersecurity Act of 2015, which was enacted in December 2015, includes several significant provisions designed to facilitate the sharing of cybersecurity threat data among the government and private sector companies, and marks the end of a multi-year effort to find a compromise between industry demands for liability protection for cybersecurity information-sharing and privacy concerns regarding government access to such information.

10 What are the principal cyberactivities that are criminalised by the law of your jurisdiction?

In general, a wide variety of criminal laws touch cybersecurity one way or another. For example, federal criminal statutes address the following activities, among others:

- computer hacking;
- identity theft;
- economic espionage;
- trade secret theft;
- breaking into computer systems and accessing, modifying or deleting data;
- stealing confidential information;
- defacing internet websites; and
- flooding websites with high volumes of irrelevant internet traffic to make websites unavailable to actual customers.

11 How has your jurisdiction addressed information security challenges associated with cloud computing?

There is no overarching framework for regulation of cloud computing information security. However, companies in several economic sectors, particularly the health, financial and government contracting sectors, are subject to guidance or regulations applicable to cloud security. In general, requirements for cloud security focus on the same basic issue: cloud computing is a species of outsourcing and a company moving data to the cloud remains responsible for the secure handling of that data.

For example, HIPAA regulations require entities covered by HIPAA to execute a business associate agreement with their service providers (including cloud providers) if their service providers are being provided access to personal health records. These agreements subject the service provider to many of the same privacy and security restrictions as the initial covered entity. Similarly, the GLBA regulations and FFIEC guidance require financial services companies to exercise diligence and oversight over their third-party information technology providers, which include cloud providers.

In addition, FedRAMP is a government-wide programme that incorporates cloud computing into federal government civilian agencies' IT capabilities through the authorisation and use of certified cloud computer providers. It also provides a standardised approach to securing cloud products and services. DoD has issued its own cloud security requirements, as well as special mandatory contractual clauses for DoD cloud service providers.

12 How do your jurisdiction's cybersecurity laws affect foreign organisations doing business in your jurisdiction? Are the regulatory obligations the same for foreign organisations?

Foreign organisations that do business in the United States are generally subject to state and federal laws to the same extent as US businesses operating in the same jurisdictions and collecting information about US individuals.

Best practice

13 Do the authorities recommend additional cybersecurity protections beyond what is mandated by law?

The NIST Cybersecurity Framework, issued in response to direction from Executive Order 13636, Improving Critical Infrastructure Cybersecurity, provides voluntary cybersecurity standards for protecting private sector computer networks owned or operated by critical infrastructure entities. NIST issued the first version of the Cybersecurity Framework in February 2014.

The Framework is divided into three parts: Framework Core, Implementation Tiers and Framework Profile. The Framework Core is designed to identify key cybersecurity activities common across all critical infrastructure networks. These are activities that companies should address when creating programs to protect critical computer systems and that identify best practices for communicating risks throughout an organisation. Specifically, the Framework Core consists of five functions designed to provide company decision-makers with a strategic view of cybersecurity risk management: identify, protect, detect, respond and recover.

For each function, the Framework identifies existing technical standards from NIST and other standards bodies to serve as 'informative references' in support of the technical implementation of the functions.

The Implementation Tiers provide context on how an organisation views cybersecurity risk and the processes in place to manage that risk. The Tiers range from Partial (Tier 1) to Adaptive (Tier 4) and describe an increasing degree of rigour and sophistication in cybersecurity risk management practices based on the business needs of the organisation.

The Framework Profile is intended to help organisations 'establish a roadmap' for prioritisation of organisational efforts to reduce cybersecurity risks. Organisations are encouraged to focus on identifying and eliminating gaps between the 'Current Profile,' which identifies cybersecurity outcomes currently being achieved, and the 'Target Profile', which indicates the outcomes needed to achieve cybersecurity risk management goals.

14 How does the government incentivise organisations to improve their cybersecurity?

There have been numerous legislative proposals to develop incentives for organisations to improve their cybersecurity, including tying adoption of standards to incentives such as grants and streamlined regulation, or using tax credits, but, so far, these initiatives have not been passed or implemented.

The Cybersecurity Act of 2015, which was enacted in December 2015, includes several significant provisions designed to facilitate the sharing of cybersecurity threat data among the government and private sector companies, and marks the end of a multi-year effort to find a compromise between industry demands for liability protection for cybersecurity information-sharing and privacy concerns regarding government access to such information. Among other things, the Act provides liability protection for private sector entities to:

- monitor their own information systems, the information systems of another entity (with authorisation), and information on those information systems;
- operate 'defensive measures' applied to an entity's own information systems or the information systems of another entity (with authorisation); and
- share and receive cyberthreat indicators or defensive measures from other entities, with no duty to warn or act based on information received.

15 Identify and outline the main industry standards and codes of practice promoting cybersecurity. Where can these be accessed?

There are several cybersecurity standards applicable to specific industries. Of note are:

- the NIST Cybersecurity Framework, which establishes a voluntary standard for promoting cybersecurity. It can be accessed at www.nist.gov/cyberframework/;
- for financial institutions, the FFIEC has issued an Information Security Handbook that outlines audit guidelines for reviewing financial institutions' security practices, effectively providing best practices to protect against security breaches. It can be accessed at http://ithandbook.ffiec.gov/it-booklets/information-security.aspx;
- the PCI-DSS establish standards applicable to merchants or vendors that process payment card data. The current version of these standards (version 3.1, adopted in April 2015) can be found at www.pcisecuritystandards.org/documents/PCI_DSS_v3-1.pdf; and
- a recently enacted set of standards applicable to certain defence contractors was established in late 2015 through amendments to the DFARS, which mandates the use of cybersecurity-related contract clauses in all DoD contracts. This new rule, which includes requirements with respect to security controls and cyber incident reporting, has been highly criticised by industry as being overly burdensome and in need of revision. The rule is currently in effect, but it was open to a public comment period, and may be changed through the standard regulatory process. A copy of the rule can be found at www.gpo.gov/fdsys/pkg/FR-2015-10-02/pdf/2015-24296.pdf.

16 Are there generally recommended best practices and procedures for responding to breaches?

Guidance from NIST and other independent organisations generally recommend several key actions immediately after learning of a data security breach. Communication is of particular importance, both among company leadership and with key constituencies. Effective breach response often includes an incident response team made up of forensic exports and key personnel who can address legal, public relations, investor relations and SEC, insurance, IT, audit and customer concerns. Most breaches require a coordinated effort to gather the facts through forensic analysis. At the same time, company leaders may need to develop a strategy to respond to the incident. Outside experts often serve important roles in this regard. External counsel can help guide the response to a breach and can structure a forensic investigation in a manner that preserves legal privileges. Outside forensic experts may be necessary to bring special skills to the response and to ensure that company personnel have appropriate resources to address the situation.

17 Describe practices and procedures for voluntary sharing of information about cyberthreats in your jurisdiction. Are there any legal or policy incentives?

The Cybersecurity Act of 2015, which was enacted in December 2015, includes several significant provisions designed to facilitate the sharing of cybersecurity threat data among the government and private sector companies, and marks the end of a multi-year effort to find a compromise between industry demands for liability protection for cybersecurity information-sharing and privacy concerns regarding government access to such information.

The Defense Industrial Base (DIB) Voluntary Cyber Security and Information Assurance programme is a voluntary cybersecurity information-sharing programme between DoD and eligible DIB companies. Companies in the programme receive certain threat information in return for sharing information regarding network intrusions that could compromise critical DoD programmes and missions. The rule establishing this programme was recently modified to conform with the newly issued DFARS rule (though, as with the DFARS rule, these changes were subject to comment and may be revised through the normal regulatory process).

Several industries have developed information sharing and analysis centres (ISACs) designed to share intelligence on cyber incidents, threats, vulnerabilities and associated responses present throughout the industries. The National Council of ISACs recognises the following centres: aviation, defence industrial base, emergency services, electric sector, financial services, information technology, maritime security, multi-state, communications, national health, nuclear, oil and gas, public transit, real estate, research and education, supply chain, surface transportation and water. In the wake of the recent increase in retail breaches, a new retail ISAC has also been established. US law firms and the automotive industry have also recently announced the establishment of industry ISACs.

Organisations may also choose to voluntarily share information with federal and state law enforcement and the Department of Homeland Security (DHS) to aid in the investigation and prosecution of criminal cybersecurity attacks.

18 How do the government and private sector cooperate to develop cybersecurity standards and procedures?

DHS, the Federal Bureau of Investigation (FBI), and DoD all have established information-sharing programs aimed at encouraging the private sector to share information about cyberthreats, such as indicators of compromise. Likewise, the NIST Framework is intended to be a voluntary, industry-led standard that applies to all critical infrastructure sectors. In developing the framework, NIST issued a draft framework, engaged with stakeholders at cybersecurity framework workshops and solicited feedback and suggestions for the final framework. NIST continues to update and improve the framework as industry provides feedback on implementation. Additionally, the Cybersecurity Act of 2015, which was enacted in December 2015, includes several significant provisions designed to facilitate the sharing of cybersecurity threat data among the government and private sector companies, and marks the end of a multi-year effort to find a compromise between industry demands for liability protection for cybersecurity information-sharing and privacy concerns regarding government access to such information.

19 Is insurance for cybersecurity breaches available in the jurisdiction and is such insurance common?

Insurance for cybersecurity breaches is available in the United States, and is becoming far more common for companies to have, particularly in the wake of judicial opinions finding that general insurance policies do not cover cybersecurity breaches. DHS has worked with public and private sector stakeholders to examine the current cybersecurity insurance market and develop solutions to advance its capacity to incentivise better cyber risk management.

Enforcement

20 Which regulatory authorities are primarily responsible for enforcing cybersecurity rules?

Enforcement of cybersecurity rules and standards falls to a variety of federal and state agencies. Various state attorneys general have initiated investigations of major data breaches and in some cases a group of US state attorneys generals have joined together to initiate multi-state investigations of data breaches. At the federal level, the US Secret Service (Electronic Crimes Task Forces and Cyber Intelligence Section), FBI and DHS play leading roles in identifying and investigating cyber breaches. The SEC also requires disclosure of material cyber risks and incidents, and has initiated several investigations relating to cyber incidents and information security. The FTC has also investigated companies for failing to protect consumers' personal information and take reasonable cybersecurity steps. The FTC has reached over 50 settlements of enforcement actions related to the alleged failure of companies to take reasonable data security measures. HHS also has authority to investigate data breaches involving medical patient information. The US Congress has also initiated its own investigations into prominent data breaches.

21 Describe the authorities' powers to monitor compliance, conduct investigations and prosecute infringements.

US federal and state authorities have wide-ranging authorities to monitor compliance, conduct investigations and prosecute infringements under numerous state and federal statutes. This includes the authority to demand documents and testimony, pursuant to legal process and other information relating to cybersecurity incidents.

22 What are the most common enforcement issues and how have regulators and the private sector addressed them?

The most common enforcement actions are based on allegations of insufficient cybersecurity practices and failure to disclose breaches involving consumer information. The FTC has an active enforcement programme examining companies that allegedly did not take 'reasonable' steps to protect consumer information. The FTC frequently seeks long-term consent agreements with companies that impose cybersecurity obligations. Such obligations may run for decades and require companies at their own expense to take certain security steps and have outside independent audits of the companies' compliance with the consent agreement. Individual state attorneys general have also initiated investigations and obtained settlements relating to the loss of consumer data. The SEC has sent a variety of letters to corporations requesting information on past cyber incidents. The private sector has responded through the creation of best practices, and NIST released a cybersecurity framework for private industry in early 2014.

23 What penalties may be imposed for failure to comply with regulations aimed at preventing cybersecurity breaches?

The most common penalties for failing to comply with cybersecurity-related regulations are related to the entry into consent orders with the federal or state government, class action lawsuits, civil penalties and payment card industry compliance fees (designed to ensure that credit card information is securely maintained). Other potential penalties include cease and desist orders; criminal penalties; limitations on activities, functions, and operations; registration revocations; and termination of insurance.

24 What penalties may be imposed for failure to comply with the rules on reporting threats and breaches?

Penalties that may be imposed for failure to comply with the rules on reporting threats and breaches include civil enforcement penalties and monetary judgments through litigation.

25 How can parties seek private redress for unauthorised cyberactivity or failure to adequately protect systems and data?

Depending on the facts of a specific situation, parties may seek private redress under a variety of causes of action, including approximately 34 separate tort claims, 15 contract claims, and other claims based on state and federal statutes. In particular, numerous state data breach notice laws contain individual rights of action, and consumers have brought class actions in response to data breaches involving sensitive personal information.

Threat detection and reporting

26 What policies or procedures must organisations have in place to protect data or information technology systems from cyberthreats?

There are currently no policies or procedures that all organisations must have in place to protect against cyberthreats. However, there are numerous federal and state laws, regulations and mandatory standards that pertain to securing privately owned IT systems and data in the United States' critical infrastructure sectors, resulting in a patchwork of regulatory requirements organisations must follow.

For instance, organisations performing contracts requiring a security clearance from the US government generally are covered by the National Industrial Security Program and are obligated to follow the National Industrial Security Program Operating Manual (NISPOM). The NISPOM includes a wide range of information system security requirements, including identification and authentication management, passwords and scanning for malicious code. Other defence contractors and subcontractors at all tiers are also required to comply with various security requirements under the new DoD rule.

Covered entities under HIPAA must implement technical policies that allow only authorised persons to access electronic protected health information and have measures that guard against unauthorised access to electronic protected health information when it is transmitted over an electronic network.

Under the GLBA, financial institutions are required to identify and control risks to customer information and customer information systems and to properly dispose of customer information. Appropriate measures the institutions must take include access controls on customer information systems and monitoring systems and procedures to detect actual and attempted attacks on or intrusions into customer information systems.

The main example of a state law requiring companies to develop policies and procedures to protect data and systems from cyberthreat is the Massachusetts Standards for the Protection of Personal Information of Residents of the Commonwealth, which requires companies collecting personal information of Massachusetts residents to develop written information security programmes containing administrative, technical and physical safeguards that protect personal information.

27 Describe any rules requiring organisations to keep records of cyberthreats or attacks.

Currently there are no broad rules requiring all organisations to keep records of cyberthreats or attacks. Organisations within certain critical infrastructure sectors may be subject to sector-specific rules. For example, the new DoD rule requires companies to report cyber incidents affecting 'covered defence information' to DoD, and to maintain forensic evidence (including forensic images and packet captures) for 90 days in the event DoD decides to conduct a further review and requests that evidence. Additionally, companies subject to the PCI-DSS are required to maintain certain log and other forensic data for a period of time to facilitate forensic review and audit.

Because cybersecurity breaches may require disclosure and result in litigation or regulatory enforcement, organisations should be aware that they may be required to provide forensic evidence and information about any such attacks. Organisations should maintain records accordingly (consistent with standard preservation practices).

28 Describe any rules requiring organisations to report cybersecurity breaches to regulatory authorities.

Numerous federal and state regulations require organisations to report cybersecurity breaches to regulatory authorities.

Public companies may be required to disclose, through public filings with the SEC, material breaches that affect the company's products, services, relationships with customers or suppliers, competitive conditions or financial controls.

Defence contractors with 'covered defence information' on their systems that experience a cybersecurity breach must report the breach to DoD.

Organisations covered by HIPAA are required to notify the Secretary of HHS following a breach of unsecured protected health information.

Most states also have enacted state data breach notice legislation, many of which require organisations to notify state attorneys general and other state regulatory agencies of security breaches involving sensitive

personally identifiable information that affect individuals in the state. Many of these states also require additional notice to individuals and, at times, the media, consumer credit reporting agencies, or both, of certain breaches that result in the loss of personally identifying information.

29 What is the timeline for reporting to the authorities?

Public companies may disclose material breaches to the SEC through a Form 8-K, the 'current report' companies must file with the SEC to announce major events that shareholders should know about. Depending on timing, these breaches may instead be reported in typical quarterly or annual securities filings.

For breaches that affect covered defence information, reports must be sent to DoD via http://dibnet.dod.mil/ within 72 hours of discovery of any cyber incident and must include specific, detailed data about the nature of the intrusion and any government projects possibly implicated. For breaches related to unsecured protected health information that affect 500 or more individuals, HIPAA-covered organisations are required to notify the Secretary of HHS without unreasonable delay, and in any case no later than 60 days after a breach. For breaches that affect fewer than 500 individuals, the Secretary may be notified of such breaches on an annual basis.

For notification to states regarding breaches affecting individuals in that state, most state laws require notification be made without undue delay and in the most expedient time possible, though some states include specific time frames.

Companies may also report breaches to law enforcement agencies, which the FTC has stated will be regarded favourably when considering whether to bring an enforcement action against a company.

30 Describe any rules requiring organisations to report threats or breaches to others in the industry, to customers or to the general public.

Most states require organisations to report security breaches involving personally identifiable information to individuals whose information was affected. Each state has its own rules, but typical requirements include that the notification be made in writing in the most expedient time possible. At the federal level, HIPAA and the GLBA require covered entities to report breaches of sensitive health or financial information, respectively. Many state data breach laws include an exception for entities complying with these federal obligations.

Update and trends

Legislators and regulators in the United States remain keenly focused on improving cybersecurity of critical infrastructure systems that are largely perceived as too vulnerable to cyberthreats. Although pressure will continue to grow to establish more uniform and clear cybersecurity standards, a consensus on how to craft such standards is likely to remain elusive. Some political leaders are advocating for regulatory mandates, and others are looking for industry-driven solutions to cybersecurity challenges. In the absence of any broad consensus for how to establish better cybersecurity standards, Federal agencies in the United States are likely to continue efforts to craft more aggressive cybersecurity regulatory requirements applicable to particular economic sectors, such as recent DoD efforts in the United States to impose far-reaching cybersecurity standards on companies operating in the defence sector. Legislative action in the near term will almost certainly steer clear of establishing mandatory cybersecurity requirements, and will instead focus on creating incentives for private sector entities to share cyberthreat data more freely with one another and with the government.

WILMERHALE®

Benjamin A Powell **benjamin.powell@wilmerhale.com**
Jason C Chipman **jason.chipman@wilmerhale.com**
Leah Schloss **leah.schloss@wilmerhale.com**

1875 Pennsylvania Ave, NW
Washington, DC 20006
United States

Tel: +1 202 663 6000
Fax: +1 202 663 6363
www.wilmerhale.com

Getting the Deal Through

Acquisition Finance
Advertising & Marketing
Air Transport
Anti-Corruption Regulation
Anti-Money Laundering
Arbitration
Asset Recovery
Aviation Finance & Leasing
Banking Regulation
Cartel Regulation
Class Actions
Construction
Copyright
Corporate Governance
Corporate Immigration
Cybersecurity
Data Protection & Privacy
Debt Capital Markets
Dispute Resolution
Distribution & Agency
Domains & Domain Names
Dominance
e-Commerce
Electricity Regulation
Enforcement of Foreign Judgments
Environment & Climate Regulation
Executive Compensation & Employee Benefits
Foreign Investment Review
Franchise
Fund Management
Gas Regulation
Government Investigations
Healthcare Enforcement & Litigation
Initial Public Offerings
Insurance & Reinsurance
Insurance Litigation
Intellectual Property & Antitrust
Investment Treaty Arbitration
Islamic Finance & Markets
Labour & Employment
Licensing
Life Sciences
Loans & Secured Financing
Mediation
Merger Control
Mergers & Acquisitions
Mining
Oil Regulation
Outsourcing
Patents
Pensions & Retirement Plans
Pharmaceutical Antitrust
Ports & Terminals
Private Antitrust Litigation
Private Client
Private Equity
Product Liability
Product Recall
Project Finance
Public-Private Partnerships
Public Procurement
Real Estate
Restructuring & Insolvency
Right of Publicity
Securities Finance
Securities Litigation
Shareholder Activism & Engagement
Ship Finance
Shipbuilding
Shipping
State Aid
Structured Finance & Securitisation
Tax Controversy
Tax on Inbound Investment
Telecoms & Media
Trade & Customs
Trademarks
Transfer Pricing
Vertical Agreements

Also available digitally

Online

www.gettingthedealthrough.com

Law Business Research

Cybersecurity
ISSN 2056-7685

THE QUEEN'S AWARDS FOR ENTERPRISE: 2012

LACCA
LATIN AMERICAN CORPORATE COUNSEL ASSOCIATION

Official Partner of the Latin American Corporate Counsel Association

ABA Section of International Law
Your Gateway to International Practice

Strategic Research Sponsor of the ABA Section of International Law