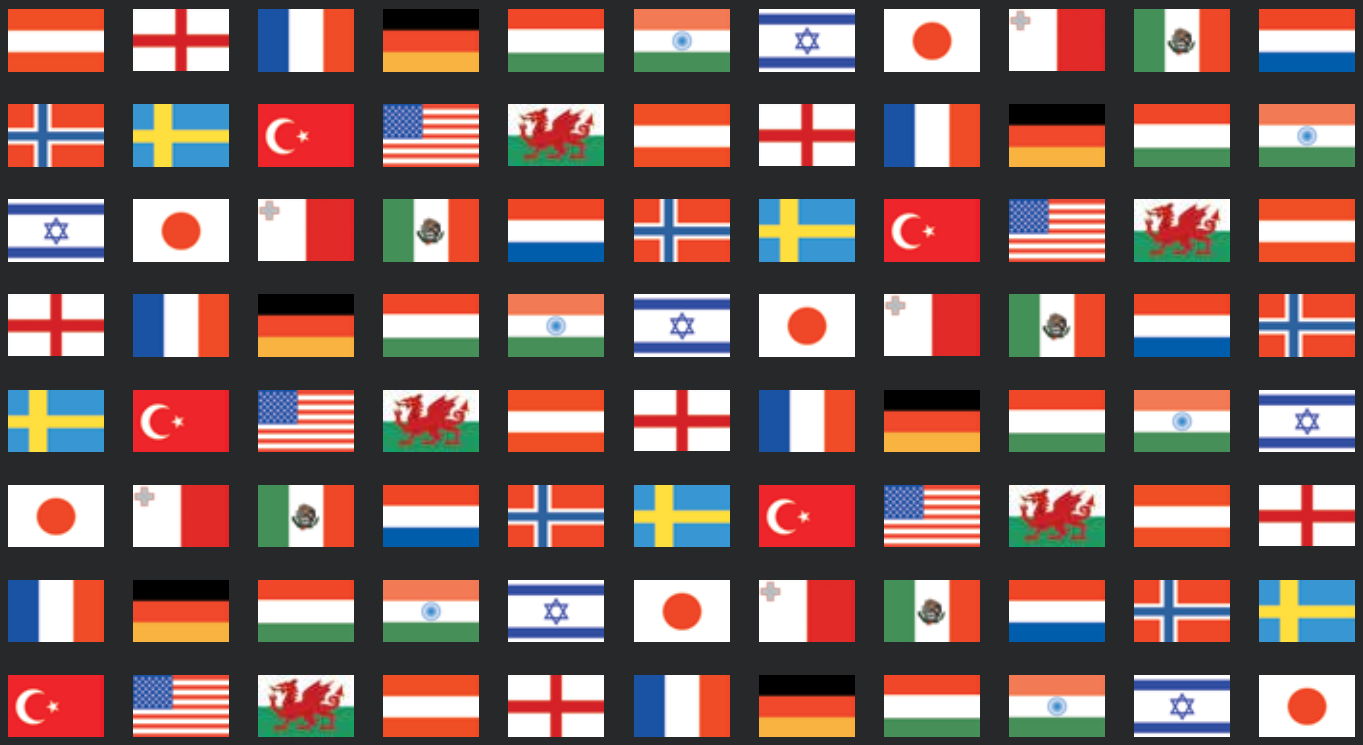
Cybersecurity

In 15 jurisdictions worldwide

Contributing editors
Benjamin A Powell and Jason C Chipman



2015

GETTING THE DEAL THROUGH

GETTING THE DEAL THROUGH

Cybersecurity 2015

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@lbresearch.com

Adam Sargent
adam.sargent@lbresearch.com

Dan White
dan.white@lbresearch.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
First edition
ISSN 2056-7685

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

CONTENTS

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 which 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 which 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 cyber- 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 (i) technical possibilities that are available; (ii) the cost of implementation; (iii) special risk involved in the processing of personal data; and (iv) 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. Furthermore, 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. Furthermore, 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 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. Furthermore, 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 address privacy and civil liberties?

Under the Swedish Constitution the right to freedom of expression and the right to privacy is granted. Everyone has the right to privacy and protection of their correspondence.

To record communication between others (where the recording party is not itself participating) is a crime under Swedish criminal statute. Such recording is allowed only if the recording party has received the consent of the participating parties. Storing of such information is regulated by the PDA. It shall be noted that wiretapping of wireless networks (eg, through radio waves) falls outside the scope of the provision (since the provision relates to older techniques available at the time the provision was drafted). However, the disclosure and passing on of such information is prohibited in accordance with the ECA.

Regarding electronic communication, providers will gain access to, for example, the content of communications. As mentioned under question 6, providers have a confidentiality undertaking regarding such information. Metadata regarding the communication may only be used for certain specified purposes. When such conditions are no longer in place, the data must be deleted.

Providers must, however, store information (such as metadata) about the communication during six months for possible access by crime preventing authorities as specified by legislation. The metadata that shall be stored are (i) information on the identity of communicating parties; (ii) when the communication took place; (iii) where the communicating parties were located; and (iv) what type of communication was used (eg, text message or telephone). The content of the communication is not saved. Information on subscription can be handed out to crime prevention authorities regardless of what crime is suspected. For other metadata, disclosure can only occur for crimes of a certain type and sanction.

The providers also have an obligation to report integrity incidents to the PTA, and to the user provided that the incident and the disclosed data may have a negative impact on the user (see question 30).

The National Defence Radio Establishment (NDRE) is the Swedish national authority for signals intelligence. The NDRE may under certain specific circumstances access private communication.

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 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 (i) assist the SCCA on information on trends regarding information security; (ii) provide opinions on the priority and conduct of the SCCA's work; (iii) perform quality certification of the SCCA's work; and (iv) 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.

17 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

18 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.

19 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.

20 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

Update and trends

One of the main challenges is the internationalisation and cross-jurisdiction transit of data and data storage. Data security will increasingly be driven and held accountable to international standards and agreements with private legal proceedings rather than local law.

The new EU Data Protection Regulation, which will strengthen data protection online, will have direct effect in Sweden. The new regulation is expected to be finalised during 2015 and thereafter the member states will be given time for adaptation. Under the new regulations, the fine for personal data breach will increase to 2 per cent of a company's global turnover. For Sweden, this will constitute a significant increase in the fines that can be issued.

Within the EU there are also ongoing initiatives regarding cybersecurity. The EU Cyber Crime Directive (2013/40/EU) was implemented in Sweden during 2014 through minor changes in criminal legislation. Sweden is also a member of the Council of Europe's Convention on Cybercrime.

In addition thereto, the European Commission has proposed a draft directive on Network and Information Security (NIS). The draft directive was adopted by the European Parliament in March 2014. The adoption of the NIS directive depends on an agreement between the EU Parliament and the EU Council on a final text.

The intention of the NIS directive is to create an overall strategy for the member states of the European Union, the infrastructure providers and operators in energy, transport, banking, etc. The directive involves measures for NIS strategies, cooperation mechanisms and risk management practices.

The European Commission has also published a cybersecurity strategy. The strategy contains the vision of the European Union on how to best prevent and respond to attacks and disruptions in the cyber environment. Specific actions are aimed at enhancing the resilience of information systems, reducing cybercrime and strengthening EU international cybersecurity policy and cyber defence.

Furthermore, the legal interpretation of the Data Retention Directive and the ECA is under discussion in Sweden. In April 2014 the Data Retention Directive (2006/24/EG) was found to be invalid by the Court of Justice of the European Communities because the data retention constituted a breach of the right to integrity and privacy. However, the Swedish government has conducted an investigation on the basis of the Court's ruling. The government found that the ECA was in proportion with the rules on privacy and integrity and would thus remain valid. On the basis of the Court's decision, some providers in Sweden ceased their own data retention under the ECA. These providers were of the opinion that the data retention rules were in breach of the rules on privacy and integrity. The PTA has issued injunctions to the providers to continue data retention according to the ECA. One provider appealed the injunction to the Administrative Court, which did not find reason to revoke the injunction.

the Data Retention Directive and the ECA must be deemed unclear (see 'Update and trends').

21 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).

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 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 21.

23 What challenges and appeals can parties make against non-compliance rulings?

Decisions made by the PTA (regarding breach of the ECA), by the DIB (regarding adherence to the PDA) and by the FSA may be appealed to the administrative court.

Note that the PTA's and DIB's statements in supervision matters cannot be appealed at all times if such statements only involve an interpretation of the legislation but do not entail a sanction towards the affected company.

24 What are the possible sanctions for cybercrimes?

For data breach the breaching party can be sentenced to fines or imprisonment for a maximum of two years. If the crime is considered gross, the sentence is at least six months to a maximum of six years' imprisonment.

For 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).

25 How can parties seek private redress for unauthorised cyber activity 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.

31 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.

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

No.

synch

Jim Runsten **jim.runsten@synchlaw.se**
Ida Häggström **ida.haggstrom@synchlaw.se**

Birger Jarlsgatan 6
PO Box 3631
103 59 Stockholm
Sweden

Tel: +46 8 761 35 35
www.synchlaw.se

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
Climate Regulation
Construction
Copyright
Corporate Governance
Corporate Immigration
Cybersecurity
Data Protection & Privacy
Debt Capital Markets
Dispute Resolution
Domains & Domain Names
Dominance
e-Commerce
Electricity Regulation
Enforcement of Foreign Judgments
Environment
Foreign Investment Review
Franchise
Gas Regulation
Government Investigations
Insurance & Reinsurance
Insurance Litigation
Intellectual Property & Antitrust
Investment Treaty Arbitration
Islamic Finance & Markets
Labour & Employment
Licensing
Life Sciences
Mediation
Merger Control
Mergers & Acquisitions
Mining
Oil Regulation
Outsourcing
Patents
Pensions & Retirement Plans
Pharmaceutical Antitrust
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
Ship Finance
Shipbuilding
Shipping
State Aid
Tax Controversy
Tax on Inbound Investment
Telecoms & Media
Trade & Customs
Trademarks
Transfer Pricing
Vertical Agreements

Also available digitally

Online

www.gettingthedealthrough.com

iPad app

Available on iTunes

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