

---

CHAMBERS GLOBAL PRACTICE GUIDES

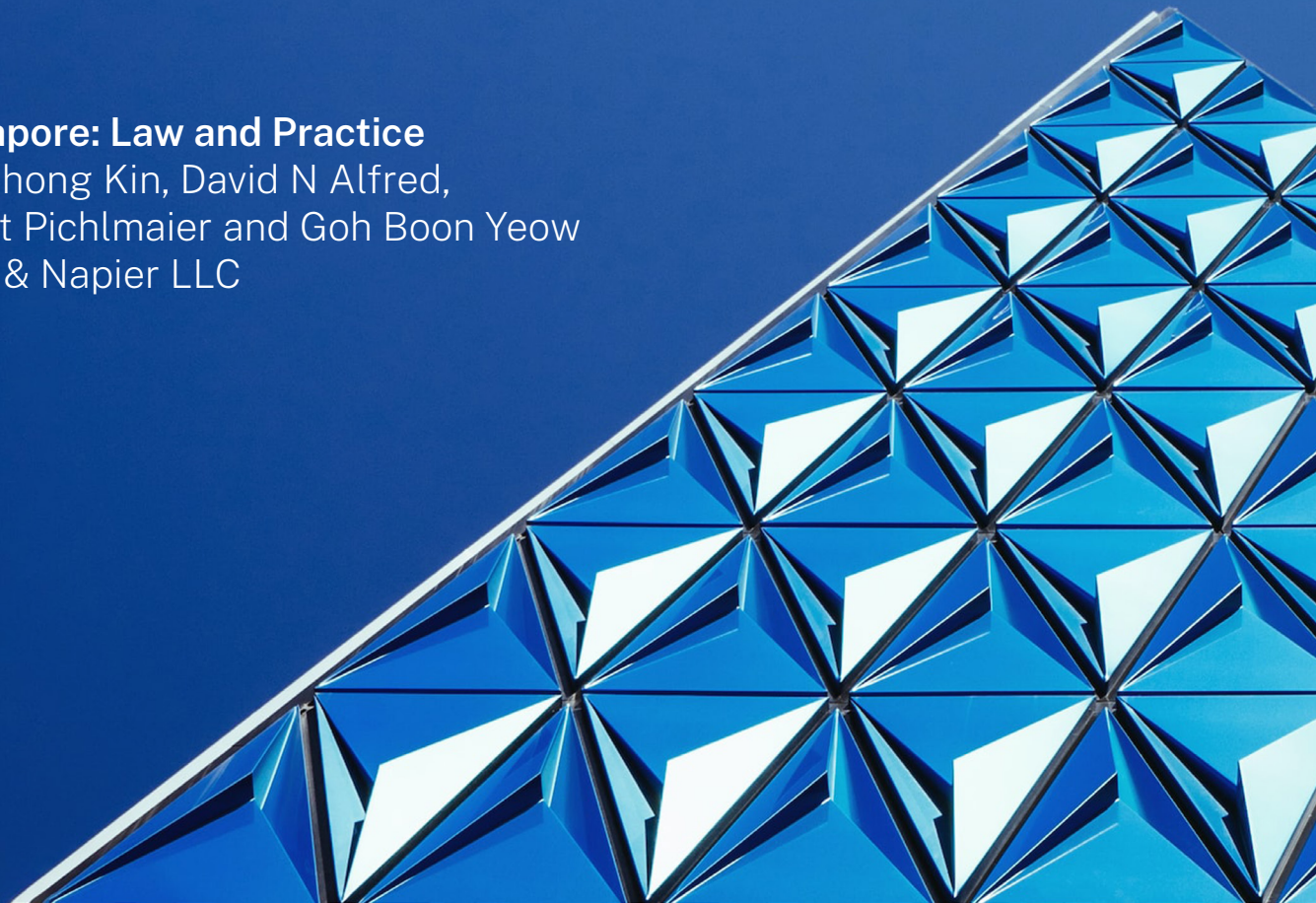
---

# Cybersecurity 2026

---

Definitive global law guides offering  
comparative analysis from top-ranked lawyers

**Singapore: Law and Practice**  
Lim Chong Kin, David N Alfred,  
Albert Pichlmaier and Goh Boon Yeow  
Drew & Napier LLC



# SINGAPORE



## Law and Practice

### Contributed by:

Lim Chong Kin, David N Alfred, Albert Pichlmaier and Goh Boon Yeow  
**Drew & Napier LLC**

## Contents

### 1. General Overview of Laws and Regulators p.4

- 1.1 Cybersecurity Regulation Strategy p.4
- 1.2 Cybersecurity Laws p.5
- 1.3 Cybersecurity Regulators p.7

### 2. Critical Infrastructure Cybersecurity Regulation p.8

- 2.1 Scope of Critical Infrastructure Cybersecurity Regulation p.8
- 2.2 Critical Infrastructure Cybersecurity Requirements p.8
- 2.3 Incident Response and Notification Obligations p.9
- 2.4 State Responsibilities and Obligations p.10

### 3. Operational Resilience in the Financial Sector p.10

- 3.1 Scope of Financial Sector Operational Resilience Regulation p.10
- 3.2 ICT Service Provider Contractual Requirements p.11
- 3.3 Key Operational Resilience Obligations p.12
- 3.4 Operational Resilience Enforcement p.12
- 3.5 International Data Transfers p.13
- 3.6 Threat-Led Penetration Testing p.13

### 4. Cyber-Resilience p.14

- 4.1 Cyber-Resilience Legislation p.14
- 4.2 Key Obligations Under Legislation p.15

### 5. Security Certification for ICT Products, Services and Processes p.15

- 5.1 Key Cybersecurity Certification Legislation p.15

### 6. Cybersecurity in Other Regulations p.15

- 6.1 Cybersecurity and Data Protection p.15
- 6.2 Cybersecurity and AI p.16
- 6.3 Cybersecurity in the Healthcare Sector p.17

**Drew & Napier LLC** established a dedicated data protection, privacy and cybersecurity practice to leverage its experience in data privacy and data and cyber governance and offer clients best-in-class solutions to address their legal and compliance needs in Singapore and across the region. The firm represents many regional and multi-national companies, industry associations, government bodies and regulators, and regularly assists them on a wide range of matters in Singapore and ASEAN member countries. At the forefront of data protection law in Singapore

since 2013, the data protection, privacy and cybersecurity practice group has worked on significant data protection enforcement cases and appeals, including those involving cybersecurity elements. Building on its experience in this field, the Drew Data Protection and Cybersecurity Academy was established in 2020 to offer clients services relating to data protection and cybersecurity compliance, including training, consulting and external Data Protection Officer services.

## Authors



**Lim Chong Kin** is the managing director of Drew & Napier's corporate and finance department, heads the telecommunications, media and technology (TMT) practice and co-heads the data protection, privacy

and cybersecurity practice. With his strong background in competition, data protection and technology laws, Chong Kin offers clients expert commercial advice. He has been an external legal and regulatory adviser for the Personal Data Protection Commission of Singapore since it was established in 2013. He also played a key role advising Singapore's Infocom regulator, the Infocommunications Media Development Authority, since 1998 on the liberalisation of Singapore's telecoms, media and postal sectors and development of the competition regimes for those sectors. Chong Kin is highly regarded by his peers, clients and rivals alike for his expertise, and is consistently recommended as a leading lawyer by major international legal publications.



**David N Alfred** is a director of Drew & Napier and co-head of the firm's data protection, privacy and cybersecurity practice group. He is concurrently co-head and programme director of the Drew Data Protection and

Cybersecurity Academy. David is a senior technology lawyer with over 25 years' experience advising on matters relating to digital technology, telecommunications and the internet. He has

substantial experience advising on data law and policy including areas such as data privacy, data protection management, data breaches cybersecurity compliance, AI governance and international aspects of data protection. David was previously the first chief counsel of Singapore's data protection authority, the Personal Data Protection Commission.



**Albert Pichlmaier** is a senior cybersecurity and privacy engineer with Drew & Napier and concurrently senior learning technology designer of the Drew Data Protection and Cybersecurity Academy. Albert is an

IT professional with over 30 years of international experience in the private and public sectors. He has worked in a wide range of IT and security domains, from smart card firmware development and test automation to AI and blockchain development, as well as IT security product certifications. Albert holds a degree in computer science and the AIGP, CISSP and CDPSE certifications. Prior to joining the firm, Albert worked for over ten years in the public sector in Singapore, most recently for Singapore's data protection authority.



**Goh Boon Yeow** is a director of Drew & Napier's corporate and finance department. Boon Yeow's main areas of practice are technology, media and telecommunications (TMT), broadcasting, cybersecurity, data

protection and privacy, and employment law. He regularly advises leading global and local telecommunications and broadcasting companies on corporate, commercial, licensing and regulatory issues. Prior to joining Drew & Napier, Boon Yeow served in the public service as a legal counsel on an overseas scholarship, where he advised on a broad range of contentious and non-contentious issues.

## Drew & Napier LLC

10 Collyer Quay  
10th Floor  
Ocean Financial Centre  
Singapore 049315

Tel: +65 6531 4110  
Fax: +65 6535 4864  
Email: [chongkin.lim@drewnapier.com](mailto:chongkin.lim@drewnapier.com)  
Web: [www.drewnapier.com](http://www.drewnapier.com)



## 1. General Overview of Laws and Regulators

### 1.1 Cybersecurity Regulation Strategy

The Singapore Cybersecurity Strategy 2021 sets a proactive national approach to an evolving cyberthreat landscape, recognising the emergence of disruptive technologies like edge computing and quantum technologies, alongside increasingly sophisticated threat actors exploiting pervasive connectivity.

The 2021 strategy aims to proactively defend Singapore's cyberspace, simplify cybersecurity for users, advance international cybersecurity norms, and emphasises the importance of a strong cybersecurity workforce and ecosystem as key enablers of Singapore's cybersecurity. Key components of the 2021 strategy include the following.

- **Building Resilient Infrastructure:** encourage enterprises and organisations to adopt a risk management mindset (as opposed to a compliance mindset) and invest in their digital infrastructure.
- **Enabling a Safer Cyberspace:** securing digital infrastructure and support the development of a healthy digital environment, which makes it easier for everyone to secure their devices and use secure applications.
- **Enhancing International Cyber Co-operation:** advance the development and implementation of voluntary, non-binding norms, which sit alongside international law. Advocate the development and adoption of technical and interoperable standards and step up operational cooperation with international partners.
- **Developing a Vibrant Cybersecurity Ecosystem:** galvanise the cybersecurity industry and academia to develop advanced capabilities, build world-class products and services, and grow Singapore's cybersecurity market.
- **Growing a Robust Cyber Talent Pipeline:** working closely with schools to educate students in cybersecurity and nurture budding cybersecurity enthusiasts and partner with industry and institutes of higher learning to develop skills and competency frameworks for cybersecurity professionals.

In terms of cybersecurity regulation, the Cybersecurity Act 2018 (see further details at **1.2 Cybersecurity Laws**) was updated in 2024 to keep pace with changes in technology, business models and the cyberthreat landscape. In so doing, the amendments will allow the Cyber Security Agency (CSA) to extend their regulatory oversight to important systems and entities not previously covered under the Cybersecurity Act 2018, adopting a risk-based approach to regulating entities for cybersecurity. In particular, the amendments extend the Act's scope to regulate additional systems where compromise could be detrimental to Singapore's national interests to better account for new technology and business models.

## 1.2 Cybersecurity Laws

Cybersecurity and cyber-risk management in Singapore is broadly regulated by a set of overlapping pieces of legislation which address the issues of national cybersecurity, cybercrimes and personal data protection. In addition, certain sectoral regulators are empowered to directly address cybersecurity issues in their respective sectors through regulatory codes, guidelines, notices, and instruments.

### Cybersecurity Act 2018 (Cybersecurity Act)

The Cybersecurity Act is the dedicated cybersecurity law which sets out the overarching framework for the oversight of national cybersecurity issues in Singapore, including the designation of computer systems (physical and virtual) as Critical Information Infrastructure (CII) in essential sectors and co-ordinating the national response to cybersecurity incidents, amongst other things. Under the Cybersecurity Act, the Commissioner of Cybersecurity is empowered to issue binding codes of practice, standards of performance and directions to regulated entities.

The Cybersecurity Act requires owners of CII to notify the Commissioner of Cybersecurity in the event of the occurrence of certain cybersecurity incidents related to their CII. A cybersecurity incident refers to an act or activity carried out without lawful authority on or through a computer or computer system that jeopardises or adversely affects its cybersecurity or the cybersecurity of another computer or computer system.

Since 2022, the Cybersecurity Act provides for the licensing of certain cybersecurity service providers (CSPs). At present, this includes CSPs that provide penetration-testing and managed security operations centre monitoring services.

To keep up with the evolving cybersecurity threats and nature of businesses, the Cybersecurity (Amendment) Bill was passed in Singapore Parliament on 7 May 2024 to expand the CSA's oversight to new entities beyond CII owners. The four new categories of entities are:

- essential service providers who use CII owned by a third-party;
- major foundational digital infrastructure (FDI) service providers;
- entities of special cybersecurity interest (ESCI); and
- owners of systems of temporary cybersecurity concern (STCC).

Importantly, the amendments have extended the definition of CII to include any computer or computer system, whether they are physical or virtual, located wholly or partly in Singapore which may be designated as CII. Such designation may arise if the Commissioner is satisfied that the computer or computer systems are necessary for the continuous delivery of an essential service, and the loss or compromise of such systems will have a debilitating effect on the availability of the essential service in Singapore. On 31 October 2025, several key provisions of the Cybersecurity (Amendment) Act 2024 came into force. Please refer to **2.2 Critical Infrastructure Cybersecurity Requirements** for more details.

### Computer Misuse Act 1993 (CMA)

The CMA sets out the enforcement and penalty framework against perpetrators of cyber-related offences, such as the unauthorised access to and modification of computer material, unauthorised use or interception of a computer service, unauthorised obstruction of use of a computer and unauthorised disclosure of a password or access code. The CMA empowers the police and other government authorities to investigate and prosecute perpetrators of cybercrimes. Where an offence under the CMA is committed by any person outside Singapore, the person may be dealt with as

if the offence had been committed within Singapore under specific scenarios.

## **Personal Data Protection Act 2012 (PDPA)**

The PDPA applies to all private sector organisations that collect, use, disclose or otherwise process personal data (both electronic and non-electronic data). Personal data is defined as data about an individual who can be identified from that data, or from that data and other information to which the organisation has or is likely to have access.

As part of complying with the PDPA, organisations are required to make reasonable security arrangements to protect personal data in their possession or under their control to prevent (i) unauthorised access, collection, use, disclosure, copying, modification, disposal, or similar risks; or (ii) the loss of any storage device or medium on which personal data is stored. Under the PDPA, the Personal Data Protection Commission (PDPC) is empowered to issue advisory guidelines which indicate the manner in which the PDPC will interpret the provisions of the PDPA.

The PDPA also includes notification requirements in the event of a data breach (see **6.1 Cybersecurity and Data Protection**).

The Do Not Call (DNC) provisions under the PDPA regulate the sending of certain marketing messages to Singapore telephone numbers. These provisions are intended to give individuals more control over the type of marketing messages they may receive by allowing individuals to register their telephone numbers with the DNC Registry and imposing obligations on organisations in respect of sending marketing messages. This thereby reduces the number of unsolicited messages received by individuals and the risk of being exposed to cybersecurity attacks.

## **Spam Control Act 2007 (SCA)**

The SCA provides for the control of spam and for matters connected with spam in Singapore. The SCA generally regulates the sending of electronic messages with a Singapore link and contains specific obligations relating to senders of unsolicited commercial electronic messages in bulk. The SCA also prohibits the sending of an electronic message to an electron-

ic address obtained through the use of a dictionary attack or address-harvesting software. The SCA is a civil penalty regime where non-compliance with these requirements may result in civil actions against the spammer.

## **Public Sector (Governance) Act 2018 (PSGA)**

Aside from the confidentiality and secrecy provisions found across various legislation, data protection and management in the public sector is also governed under the PSGA. The PSGA imposes criminal penalties on public officers who recklessly or intentionally disclose data without authorisation, misuse data for a gain or re-identify anonymised data. Specific data security policies are further set out in the Government Instruction Manual on IT Management.

## **Other Sectoral Frameworks**

Two notable examples are in the telecommunications and banking and finance sectors.

First, the telecoms and media regulator, the Info-communications Media Development Authority (IMDA), has published a Telecommunications Cybersecurity Code of Practice to enhance cybersecurity preparedness of designated telecommunication licensees such as internet service providers in Singapore. This Code of Practice, which was formulated in line with international standards and best practices including the ISO/IEC 27011 and IETF Best Current Practices, sets out requirements on security incident management and other controls to help licensees prevent, protect, detect and respond to cybersecurity threats.

Second, the Singapore financial regulatory authority, the Monetary Authority of Singapore (MAS), has issued its Technology Risk Management (TRM) Guidelines (the "TRM Guidelines"), which set out risk management principles and best practices to guide financial institutions (FIs) in establishing sound and robust technology risk governance and oversight, as well as in maintaining IT and cyber-resilience. In conjunction with this, the MAS has also issued legally binding Notices on TRM and Cyber Hygiene which give effect to some of the requirements in the TRM Guidelines. Please also see **3.1 Scope of Financial Sector Operation Resilience Regulation** for further details.

## 1.3 Cybersecurity Regulators Cyber Security Agency of Singapore

The regulatory authority responsible for the administration and enforcement of the Cybersecurity Act is the CSA. The CSA is part of the Prime Minister's Office and is managed by the Ministry of Digital Development and Information (MDDI), and led by the Commissioner of Cybersecurity. The Minister for Digital Development and Information (as the Minister-in-charge of Smart Nation and Cybersecurity) may appoint Assistant Commissioners from sectoral regulators who understand the unique context and complexity of their respective sectors to advise and assist the Commissioner on the co-ordination of cybersecurity efforts.

Under the Cybersecurity Act, the Commissioner's functions and duties include, but are not limited to:

- advising the Singapore government or any other public authority on cybersecurity matters;
- monitoring and responding to cybersecurity threats, whether such cybersecurity threats occur in or outside Singapore;
- identifying, designating and regulating provider-owned CII, designated providers responsible for third-party-owned CII and STCC;
- establishing cybersecurity codes of practice and standards of performance for implementation by owners of provider-owned CII, designated providers responsible for third-party-owned CII and STCC;
- developing and promoting the cybersecurity services industry in Singapore; and
- licensing and establishing standards in relation to CSPs.

In general, the Cybersecurity Act applies to any computer or computer system, whether physical or virtual, and located wholly or partly in Singapore which may be designated as CII. The Commissioner may confer such a designation when satisfied that the computer or computer systems are necessary for the continuous delivery of an essential service, and the loss or compromise of such systems will have a debilitating effect on the availability of the essential service in Singapore.

Where an essential service provider relies on third-party-owned computers or computer systems that

are necessary for delivering the essential service, the Commissioner may designate the provider as responsible for the cybersecurity of that third-party-owned CII, and the provider must ensure comparable cybersecurity standards through legally binding commitments.

If the risk of a cyber-attack is high and the loss or compromise of the computer or computer system will have a serious detrimental effect on the national security, defence, foreign relations, economy, public health, public safety or public order of Singapore, the Commissioner may designate the computer or computer system as a STCC, and subject the STCC to obligations similar to CII.

The Cybersecurity Services Regulation Office (CSRO) was set up within the CSA in 2022 to administer the licensing framework of CSPs under the Cybersecurity Act, responding to the industry's queries and feedback, and sharing of resources on licensable cybersecurity services.

Currently, there are 11 sectors in which there may be essential services (ie, services which are essential to national security, defence, foreign relations, the economy, public health, public safety or the public order of Singapore):

- energy;
- info-communications;
- media;
- water;
- healthcare;
- banking and finance;
- security and emergency services;
- aviation;
- land transport;
- maritime; and
- services relating to the functioning of the government.

The Commissioner has broad powers to investigate and prevent cybersecurity threats or incidents, including making requests for information to be provided or, in serious cases, direct remedial measures to be taken by any person (including those who are not owners of CII).

The CSA operates the Singapore Cyber Emergency Response Team (SingCERT), which is Singapore's national cyber-incident response team for its constituents. SingCERT facilitates the detection, resolution and prevention of cybersecurity-related incidents and provides a public channel for incident reporting.

## Personal Data Protection Commission

The PDPC was established in January 2013 as Singapore's data protection authority. It is under the purview of the MDDI and tasked with enforcing and administering the PDPA. The PDPC is led by the Commissioner for Personal Data Protection. Please refer to **1.2 Cybersecurity Laws**.

The PDPA confers powers on the PDPC to enforce the PDPA, which include powers relating to:

- alternative dispute resolution (eg, mediation);
- reviews of data subjects' access and correction requests;
- investigations to ensure compliance with the PDPA (including the DNC provisions); and
- voluntary undertakings.

## 2. Critical Infrastructure Cybersecurity Regulation

### 2.1 Scope of Critical Infrastructure Cybersecurity Regulation

Please refer to **1.2 Cybersecurity Laws** and **1.3 Cybersecurity Regulators**.

### 2.2 Critical Infrastructure Cybersecurity Requirements

Generally, owners of CII are required to comply with a set of general duties, such as:

- comply with notices issued by the Commissioner to provide information on the technical architecture of the CII;
- comply with codes of practice, standards of performance or written directions in relation to the CII;
- notify the Commissioner of any change in ownership of the CII;

- notify the Commissioner of any prescribed cybersecurity incidents (please refer to **2.3 Incident Response and Notification Obligations**);
- conduct regular audits of the compliance of the CII with the Cybersecurity Act, codes of practice and standards of performance;
- conduct regular risk assessments of the CII as required by the Commissioner; and
- participate in cybersecurity exercises as required by the Commissioner.

The Cybersecurity Code of Practice for Critical Information Infrastructure (the "CII Cybersecurity Code") requires owners of CII to put in place security baseline configuration standards for all operating systems, applications and network devices of a piece of CII that is commensurate with the cybersecurity risk profile of that CII. The security baseline configuration standards address the following security principles:

- least access privilege and separation of duties;
- enforcement of password complexities and policies;
- removal of unused accounts;
- removal of unnecessary services and applications (eg, removal of compilers and vendor support applications);
- closure of unused network ports;
- protection against malware; and
- timely update of software and security patches that are approved by system vendors.

Following the commencement of the Cybersecurity (Amendment) Act, the Cybersecurity Act has been updated to cover four additional classes of entities.

- Designated providers of essential services that do not own the CII used for the continuous delivery of the essential services they are responsible for (third-party-owned CII): the providers of such essential services are required to obtain legally binding commitments from the third-party to provide the necessary information or adhere to prescribed standards relating to cybersecurity, etc. The Commissioner may order such providers to cease using the third-party-owned CII if they do not obtain the legally binding commitments (in effect as of 31 October 2025).

- Owners of computers or computer systems designated as STCC: for example, the temporary systems used to support the distribution of critical vaccines during a pandemic could fall under this category (in effect as of 31 October 2025).
- Designated entities of special cybersecurity interest (ESCI): if the function of such designated entities perform is disrupted, or if the sensitive information contained in their computer systems is disclosed, there will be a significant detrimental effect on the defence, foreign relations, economy, public health, public safety or public order of Singapore; (to come into effect at a later date).
- Designated providers of major foundational digital infrastructure services (FDI): these services promote the availability, latency, throughput or security of digital services, and relate to cloud computing services and data facility services (to come into effect at a later date).

The amendments to the Cybersecurity Act impose obligations on these new entities that are similar to those already in force relating to CII, such as:

- providing the Commissioner with information;
- complying with any codes of practice, standards of performance or written directions that may be issued or approved by the Commissioner; and
- notifying the Commissioner of any prescribed cybersecurity incident.

## 2.3 Incident Response and Notification Obligations

Under the Cybersecurity (Provider-Owned Critical Information Infrastructure) Regulations 2018 and Cybersecurity (Systems of Temporary Cybersecurity Concern) Regulations 2025, cybersecurity incidents that must be reported to the Commissioner include:

- any unauthorised hacking of the relevant computer or computer system/STCC or the interconnected computer or computer system to gain unauthorised access to or control of the relevant computer or computer system/STCC or interconnected computer or computer system;
- any installation or execution of unauthorised software, or computer code, of a malicious nature on the relevant computer or computer system/

STCC or the interconnected computer or computer system;

- any man-in-the-middle attack, session hijack or other unauthorised interception by means of a computer or computer system of communication between the relevant computer or computer system/STCC or the interconnected computer or computer system, and an authorised user of the relevant computer or computer system/STCC or the interconnected computer or computer system as the case may be; and
- any denial of service attack or other unauthorised act or acts carried out through a computer or computer system that adversely affects the availability or operability of the relevant computer or computer system/STCC or the interconnected computer or computer system.

Since 31 October 2025, incident reporting for owners of CII was expanded to include the following circumstances, where the CII owner:

- becomes aware that the cybersecurity incident has any effect which is observable by any member of the public;
- becomes aware that the cybersecurity incident was caused by or related to an exploitation of a vulnerability which was a zero-day vulnerability at the time of the exploit;
- becomes aware that any indicator of compromise that is associated with an advanced persistent threat and was previously notified in writing to the CII owner by the Commissioner of Cybersecurity was detected in relation to the cybersecurity incident; and
- suspects that the cybersecurity incident may have been caused by an advanced persistent threat.

The competent supervisory authority for the CII incident notification regime is the Commissioner of Cybersecurity within the CSA. The CII owner must submit an initial report (with the prescribed details) of the cybersecurity incident or occurrence of one of the above-mentioned circumstances within two hours after the occurrence of the cybersecurity incident or circumstance. This notification must be made by calling the telephone number specified by the Commissioner.

Where the owner of the CII is unable to submit the prescribed details via calling the specified telephone number within a reasonable time, the owner may provide the details by text message to the specified telephone number or in writing via the form on CSA's website.

Supplementary details of the cybersecurity incident/circumstance must be provided in writing in the form set out on CSA's website within 72 hours after becoming aware of such occurrence. This includes any updates and supplementary details following from the initial notification, the cause of the cybersecurity incident, the impact of the cybersecurity incident and what remedial measures have been taken.

A final incident report containing all the details in the initial notification and supplementary details (and any updates thereto) must be submitted via the form on CSA's website within 30 days after the submission of the supplementary details.

Sections 16I(1) and 17E(1) of the Cybersecurity Act also impose similar reporting obligations on designated providers responsible for third-party-owned CII and owners of STCCs.

When the new Parts 3C and 3D under the Cybersecurity (Amendment) Act are brought into force, there will be reporting obligations imposed on ESCIs and major FDI service providers as well.

A single cyber-incident may trigger parallel reporting obligations under other regulatory regimes, depending on the nature of the affected information and the regulated sector. If the incident involves a notifiable personal data breach, the organisation may also have to notify the PDPC within the statutory timeline and, where required, notify affected individuals.

## 2.4 State Responsibilities and Obligations

Under Section 5 of the Cybersecurity Act, the Commissioner of Cybersecurity has a duty to monitor cybersecurity threats in or outside of Singapore, advise the government or any other public authority on the national needs and policies in respect of cybersecurity matters generally, and respond to cybersecurity incidents that threaten the national security, defence,

economy, foreign relations, public health, public order or public safety, or any essential services of Singapore, whether such cybersecurity incidents occur in or outside Singapore, among other duties.

Additionally, SingCERT routinely issues cybersecurity and cyber-hygiene advisories and alerts. SingCERT also works with the sectoral regulators to issue relevant alerts and advisories to industry players and to inform companies and affected individuals on cybersecurity threats and incidents.

The CSA has established programmes to raise baseline cyber-resilience across the economy and institutionalise engagement with industry partners. The SG Cyber Safe Programme provides structured support for organisations to strengthen cybersecurity, and the SG Cyber Safe Partnership Programme is intended to mobilise industry partners to develop training content, products, services and outreach initiatives that encourage adoption of good cybersecurity practices.

## 3. Operational Resilience in the Financial Sector

### 3.1 Scope of Financial Sector Operational Resilience Regulation

Please refer to **1.2 Cybersecurity Laws** for a summary of the sectoral cybersecurity laws applicable to the banking and finance sector.

In the banking and finance sector, the MAS has issued a set of legally binding Notices on TRM and Cyber Hygiene which apply to FIs (eg, banks, insurers, capital markets services licence holders, operators, and settlement institutions of designated payment systems). These Notices impose obligations on FIs to enhance information security and mitigate the growing risks of cyberthreats.

The TRM Notices include requirements to:

- put in place a framework and process to identify critical systems;
- make reasonable efforts to maintain a high availability of critical systems;

- establish a recovery time objective for each critical system;
- notify the MAS of a system malfunction or IT security incident;
- submit a root cause and impact analysis report to the MAS of the relevant incident within 14 days; and
- implement IT controls to protect customer information from unauthorised access or disclosure.

The Notices on Cyber Hygiene include requirements to:

- secure administrative accounts;
- apply security patching;
- establish baseline security standards;
- deploy network perimeter defences;
- implement anti-malware measures; and
- strengthen multi-factor authentication.

The MAS has also published Guidelines on Outsourcing for banks and other FIs, which set out the MAS's expectations of entities that have entered into an arrangement for ongoing outsourced services which are obtained or received by the bank/FI. The guidelines list measures which include requiring the relevant entities to conduct due diligence, maintain ongoing oversight, and implement contractual safeguards that preserve auditability and supervisory access.

### 3.2 ICT Service Provider Contractual Requirements

Under the TRM Guidelines, MAS sets out principles and best practices to in relation to third-party service providers, which include:

- ensuring service providers have the requisite level of competence and skills to perform IT functions and manage technology risks;
- conducting IT security awareness training programmes for service providers who have access to FIs' information assets;
- identifying threats and vulnerabilities applicable to information assets that are maintained or supported by service providers;
- assessing service providers' disaster recovery capability and ensuring that disaster recovery

- arrangements are established, tested and verified to meet FIs' business needs;
- ensuring service providers are accorded the same level of protection and subject to the same security standards in data security as FIs;
- involving service providers in scenario-based cyber exercises to validate FIs' response and recovery, as well as communication plans against cyber threats; and
- reporting of phishing attempts to service providers.

Under the MAS Guidelines on Outsourcing, MAS expects banks/FIs to conduct a self-assessment of their existing outsourcing arrangements against the several risk management practices, including (non-exhaustive):

- carefully defining terms and conditions in outsourcing agreements governing relationships, obligations, responsibilities, rights and expectations of parties;
- retaining the ability to monitor and control risks when using sub-contractor(s);
- establishing a structure for monitoring and control of outsourcing arrangements;
- taking into account prescribed factors in risk management when outsourcing outside Singapore; and
- requiring the board and senior management to provide information on structure and processes when outsourcing within a group.

ICT service providers may fall under the upcoming category of designated providers of major FDI services under the Cybersecurity Act. "FDI services" are services that promote the availability, latency, throughput or security of digital services, and will be specified in the Third Schedule to the Cybersecurity Act once these provisions under the Cybersecurity (Amendment) Act come into force. This will include "cloud computing service" and "data centre facility service" (as defined under the Act).

Once these provisions under the Cybersecurity (Amendment) Act come into force, designated providers of major FDI services will be subject to obligations such as providing the Commissioner with information, reporting prescribed cybersecurity incidents,

and complying with codes of practices and directions that may be issued or approved by the Commissioner.

### 3.3 Key Operational Resilience Obligations

The key obligations relating to governance and risk management can be derived from Part 3 and 4 of the TRM Guidelines relating to Technology Risk Governance and Oversight. The best practices that FIs should aim to comply with include (non-exhaustive):

- ensuring that the board of directors and senior management implement effective internal controls and risk management practices;
- ensuring that the board of directors and senior management have members with sufficient knowledge to understand and manage technology risks;
- establishing and implementing a technology risk management strategy, and ensuring key IT decisions are made in accordance with the FI's risk appetite; and
- maintaining up-to-date technology risk policies, standards and procedures, with compliance monitoring and disciplined management of deviations through approved risk assessments.

The key obligations relating to digital operation resilience generally in the financial sector can be derived from Part 8 of the TRM Guidelines relating to IT resilience. The best practices that FIs should aim to comply with include (non-exhaustive):

- establishing system availability commensurate with their business needs;
- establishing system recoverability aligned to their business resumption and system recovery priorities; and
- regularly testing their disaster recovery plans to validate their effectiveness and ensure that they meet the defined recovery objectives.

FIs should establish cyber-incident response and management plans to swiftly isolate and neutralise cyber threats and to securely resume affected services. The plan should describe communication, co-ordination and response procedures to address plausible cyber threat scenarios. Each FI should seek to understand their exposure to technology risks and

place a robust risk management framework to ensure cyber-resilience.

FIs may also be a designated entity under the Cybersecurity Act. For more information on the designation of entities and their obligations under the Cybersecurity Act, please refer to **1.2 Cybersecurity Laws**, **1.3 Cybersecurity Regulators** and **2.2 Critical Infrastructure Cybersecurity Requirements**.

### 3.4 Operational Resilience Enforcement

There are no specific obligations relating to operation resilience in relation to critical ICT service providers. However, critical ICT service providers in the financial sector can take guidance from Part 8 of the TRM Guidelines (please refer to **3.3 Key Operational Resilience Obligations** for further details).

Generally, under Section 29 (1) of the Financial Services and Markets Act, MAS has the power to issue directions or make regulations concerning any FI or class of FIs as the MAS considers necessary for:

- the management of technology risks, including cyber security risks;
- the safe and sound use of technology to deliver financial services; and
- the safe and sound use of technology to protect data.

An FI that fails to comply with a direction issued to it under Section 29 (1) or contravenes any regulation mentioned in that subsection shall be guilty of an offence and shall be liable on conviction to a fine not exceeding SGD1 million and, in the case of a continuing offence, to a further fine of SGD100,000 for every day or part of a day during which the offence continues after conviction.

Under the Cybersecurity Act, the Commissioner has broad powers under Sections 19 and 20 to investigate and prevent cybersecurity incidents and “serious” cybersecurity incidents respectively. These include powers to require persons to attend interviews, require the production of relevant information, give directions to carry out remedial measures or cease activities, enter premises, access and inspect computer systems, among others.

It is an offence for any person to fail to co-operate with the CSA without reasonable excuse and such persons shall be liable on conviction to be punished in accordance with the fines, terms of imprisonment or both, as set out in the relevant statutory provisions.

Under the upcoming Section 18K(1) in Part 3D of the amended Cybersecurity Act, the Commissioner may require major FDI service providers to furnish information. If the major FDI service provider fails to, without reasonable excuse, furnish the required cybersecurity-related information within the specified period or continues providing the designated FDI service despite the non-compliance, they shall be guilty of an offence. They shall be liable for a fine not exceeding the greater of SGD200,000 or 10% of the annual turnover of the service provider's business in Singapore.

The upcoming Section 18L(1) also empowers the Commissioner to issue written instructions to major FDI service providers which may relate to the action to be taken by the provider in relation to a cybersecurity threat, compliance with any prescribed technical standards relating to cybersecurity, among others. Any major FDI service provider who fails to comply with such a written direction and continues to provide FDI infrastructure service after the deadline for compliance will be liable on conviction to a fine not exceeding the greater of SGD200,000 or 10% of the annual turnover of the person's business in Singapore.

Further, under the upcoming Section 18M (1), major FDI service providers must notify the Commissioner of the occurrence of a prescribed cybersecurity incident in respect of the major FDI, where the incident results in a disruption or degradation to the continuous delivery of the foundational digital infrastructure service or the major FDI service provider's business operations in Singapore. Any major FDI service provider who, without reasonable excuse, fails to comply with this obligation shall be guilty of an offence and liable on conviction to a fine not exceeding the greater of SGD200,000 or 10% of the annual turnover of the person's business in Singapore.

As the provisions relating to the obligations for major FDI service providers have not yet commenced, there are no enforcement decisions against major FDI ser-

vice providers for the failure to comply with the Cybersecurity Act.

### 3.5 International Data Transfers

There are no specific obligations imposed by MAS in relation to financial institutions carrying out international data transfers. However, organisations transferring personal data overseas must comply with Section 26 of the PDPA. Under Section 26, organisations need to ensure that the personal data transferred overseas is accorded a standard of protection that is comparable to the protection under the PDPA.

Under the Personal Data Protection Regulations 2021 (the "PDP Regulations"), the transferring organisation must take appropriate steps to ascertain whether, and to ensure that, the recipient of the personal data is bound by legally enforceable obligations (as defined under the PDP Regulations) to provide to the transferred personal data a standard of protection that is at least comparable to the protection under the PDPA.

Alternatively, this requirement is deemed to have been met if:

- the data subject whose personal data is to be transferred gives their consent to the transfer of their personal data, after being provided with a reasonable summary in writing of the extent to which the personal data transferred to those countries and territories will be protected to a standard comparable to the protection under the PDPA; or
- the transfer is necessary for the performance of a contract between the organisation and the data subject, or to do anything at the data subject's request with a view to his/her entering a contract with the organisation.

As good practice, organisations are encouraged to rely on the above circumstances only if they are unable to rely on legally enforceable obligations or specified certifications.

### 3.6 Threat-Led Penetration Testing Critical Information Infrastructure

Under the CII Cybersecurity Code, owners of CII are required to conduct regular penetration testing on

their own CII to identify security vulnerabilities that could be exploited by a cyber threat actor.

Owners of CII are required to conduct a penetration test on the CII at least once:

- every 12 months, for CII which is an information technology system; and
- every 24 months, for CII which is an operational technology system.

Owners of CII must conduct penetration tests on relevant CII assets after implementing any major system changes to the CII.

It is the responsibility of CII owners to ensure that third-party penetration testing service providers and their penetration testers possess industry-recognised accreditations and certifications respectively, for example CREST or equivalent accreditations and certifications.

Owners of CII are required to establish a red teaming or purple teaming attack simulation plan, and conduct a red teaming or purple teaming attack simulation on its CII at least once every 24 months.

## Cybersecurity Service Provider Licences

The Cybersecurity Services Regulation Office (CSRO) was set up to administer the licensing framework for CSPs under the Cybersecurity Act.

All providers of a managed security operations centre monitoring services and penetration testing services as defined in the Cybersecurity Act to the Singapore market must apply to the CSRO for a cybersecurity service provider's licence.

## IoT Devices

In 2020, the MDDI (then Ministry of Communication and Information) introduced the Cybersecurity Labelling Scheme (CLS). The CLS was, initially a voluntary scheme for Wi-Fi routers and smart home hubs, and was subsequently expanded to include all smart home devices.

The CLS provides four cybersecurity rating levels for registered IoT devices and other smart devices to help

consumers easily assess the level of security offered and make informed choices in purchasing a device. At Level 1, the product meets basic security requirements, whilst at Level 4, the product has undergone structured penetration tests by approved third-party test labs.

In 2024, the CSA updated Singapore's Operational Technology Cybersecurity Masterplan. It now includes operators of operational technologies that support physical control functions such as IoT and industrial IoT devices, as such devices have become new attack surfaces for threat actors to exploit. The key initiatives under the masterplan include:

- enhancing the operational technology cybersecurity talent pipeline;
- enhancing information sharing and reporting;
- uplifting operational technology cybersecurity resilience beyond CII; and
- promoting secure-by-development principles.

## 4. Cyber-Resilience

### 4.1 Cyber-Resilience Legislation

The Singapore Cybersecurity Strategy 2021 emphasises enhancing response capabilities for the state, organisations and individuals rather than expanding legislation relating to cyber-resilience (please refer to **1.1 Cybersecurity Regulation Strategy** for more details).

Apart from the Cybersecurity Act and the other legislation mentioned in **1.2 Cybersecurity Laws**, the legislative status of cyber-resilience in Singapore remains relatively sparse compared to that of other jurisdictions. Instead, security-by-design outcomes for connected products are driven through product assurance and labelling schemes, as well as technical requirements in targeted areas. Notably, the CLS is intended to incentivise manufacturers to build in stronger cybersecurity provisions. Residential gateways are also subject to IMDA technical security specifications, with compliant routers qualifying for CLS recognition.

For cloud and digital infrastructure services, the amended Cybersecurity Act introduces a framework to regulate major FDI service providers. Foundational digital infrastructure services are currently specified to include cloud computing services and data centre facility services, with definitions that expressly contemplate services delivered from systems in Singapore or outside Singapore. In addition, the government has been studying a Digital Infrastructure Act to enhance resilience and security of key digital infrastructure and services, and the IMDA has issued advisory guidelines for cloud services and data centres as interim uplift measures.

## 4.2 Key Obligations Under Legislation

Please refer to **1.2 Cybersecurity Laws**, **2.2 Critical Infrastructure Security Requirements**, **3.2 ICT Service Provider Contractual Requirements**, **3.3 Key Operational Resilience Obligations**, **3.4 Operational Resilience Enforcement** and **4.1 Cyber-Resilience Legislation**.

## 5. Security Certification for ICT Products, Services and Processes

### 5.1 Key Cybersecurity Certification Legislation

While there is no prescribed cybersecurity certification legislation in Singapore, the CSA offers, administers and supports the use of certification schemes to provide assurance to customers that the product has been objectively assessed from a cybersecurity standpoint.

The CSA Cybersecurity Certification Centre operates several schemes which cover ICT product security in general. For example, besides the CLS, the Singapore Common Criteria Scheme provides a cost-effective regime to evaluate and certify the security of IT products in Singapore against the Common Criteria (CC) standards (ie, ISO/IEC 15408 series).

The CSA also operates the National IT Evaluation Scheme. This scheme evaluates IT products for high security assurance by referencing international standards such as the CC.

The PDPC and the IMDA jointly developed the Data Protection Trustmark (DPTM) Certification to help organisations demonstrate compliance with the PDPA. The DPTM Certification also incorporates elements of international benchmarks and data protection best practices. Since 2025, the DPTM has been administered by the Singapore Accreditation Council.

## 6. Cybersecurity in Other Regulations

### 6.1 Cybersecurity and Data Protection

#### General Requirements Under the PDPA

In the context of personal data protection, organisations are required to put in place data protection policies and practices to ensure and demonstrate compliance with their obligations under the PDPA. Specifically, these requirements include:

- appointing a data protection officer to oversee compliance with the PDPA;
- developing and implementing data protection policies, practices and procedures to ensure proper processing of personal data; and
- providing adequate training to staff that handle and process personal data.

#### Protection Obligation

Under Section 24 of the PDPA, an organisation is required to make reasonable security arrangements to protect personal data in their possession or under their control.

#### Data Breach Notification

A “data breach” is defined in the PDPA to mean:

- the unauthorised access, collection, use, disclosure, copying, modification, or disposal of personal data; or
- the loss of any storage medium or device on which personal data is stored in circumstances where the unauthorised access, collection, use, disclosure, copying, modification, or disposal of the personal data is likely to occur.

Where an organisation has reason to believe that a data breach affecting personal data in its possession or control has occurred, it must conduct an assess-

ment of whether it is a “notifiable data breach” in a reasonable and expeditious manner.

A data breach is a “notifiable data breach” if the data breach (i) results in, or is likely to result in, significant harm to an affected individual; or (ii) is, or is likely to be, on a significant scale (ie, affecting at least 500 persons).

According to the Personal Data Protection (Notification of Data Breaches) Regulations 2021 (the “Data Breach Regulations”), a data breach is deemed to result in significant harm to an individual if it relates to the following:

- the individual’s full name or alias or identification number, and any of the personal data or classes of personal data relating to the individual as set out in the schedule to the Data Breach Regulations; and
- all of the following personal data relating to an individual’s account with an organisation:
  - (a) the individual’s account identifier, such as an account name or number; or
  - (b) any password, security code, access code, response to a security question, biometric data or other data that is used or required to allow access to, or use of, the individual’s account.

Upon assessing that the data breach is a “notifiable data breach”, the organisation must notify the PDPC in the prescribed form no later than three calendar days after assessment.

The organisation must also notify each individual affected by the data breach, if the data breach results in, or is likely to result in significant harm to an affected individual, unless one of the following exceptions applies:

- if, on or after assessing that the data breach is a “notifiable data breach”, the organisation takes any action that renders it unlikely that the data breach will result in significant harm to the affected individual; or
- if the organisation had implemented, prior to the occurrence of the data breach, any technological measure that renders it unlikely that the data

breach will result in significant harm to the affected individual.

Where a data intermediary processing personal data on behalf of another organisation has reason to believe a data breach has occurred, it must, without undue delay, notify the primary organisation.

## 6.2 Cybersecurity and AI

Computers or computer systems which support AI solutions may be designated as a CII (or as another designated entity) under the Cybersecurity Act if they are necessary for the continuous delivery of an essential service, and the loss or compromise of the computer or computer system will have a debilitating effect on the availability of the essential service in Singapore. Following the amendments to the Cybersecurity Act that took effect on 31 October 2025, such systems can be physical or virtual, and in certain cases, may be located outside Singapore where the statutory designation criteria are met. For further details, please refer to **1.2 Cybersecurity Laws**, **1.3 Cybersecurity Regulators** and **2.2 Critical Infrastructure Cybersecurity Requirements**.

While there are currently no express cybersecurity obligations relating to AI in Singapore, several voluntary frameworks and guidelines have been published relating to the development and use of AI.

Amongst these, the Model AI Governance Framework for Generative AI sets out a systematic and balanced approach to address generative AI concerns while facilitating innovation. It recommends adapting the “security-by-design” concept. The framework also makes recommendations regarding incident reporting. After incidents happen, organisations need internal processes to ensure timely notification and remediation of the incident. Depending on the impact of the incident and how extensively AI was involved, organisations should consider notifying both the public and the government.

On 15 October 2024, the CSA published the Guidelines and Companion Guide on Securing AI Systems (the “Guidelines on Securing AI Systems”). The Guidelines on Securing AI Systems set clear expectations that AI systems should be secure by design and by

default, and that security should be addressed holistically across the AI system lifecycle. The Guidelines on Securing AI Systems address potential security risks through the AI lifecycle and help to protect AI systems against traditional cybersecurity risks, such as supply chain attacks, as well as novel risks such as Adversarial Machine Learning. Key recommendations include taking a lifecycle approach to consider security risks, starting with a risk assessment.

Furthermore, in October 2025, the CSA launched a public consultation on Securing Agentic AI – An Addendum to the Guidelines and Companion Guide on Securing AI Systems. This addendum is meant to be read together with the Guidelines on Securing AI Systems and advises system owners on securing their agentic AI systems. It also outlines how risks can be identified and assessed based on the capabilities of agentic AI systems, and provides practical controls to mitigate relevant risks across the development lifecycle.

The Engaging with Artificial Intelligence guide, which was published on 25 January 2024 by the Australian Signals Directorate’s Australian Cyber Security Centre in conjunction with the CSA and other international agencies, also provides organisations with guidance on how to use AI systems securely. The guide summarises some important threats related to AI systems and prompts organisations to consider the steps they can take to engage with AI while managing risk. The document provides cybersecurity mitigations to assist organisations that use self-hosted and/or third-party hosted AI systems.

A Model Governance Framework for Agentic AI was published by the IMDA on 22 January 2026. The framework provides a structured overview of the risks of agentic AI and emerging best practices in managing such risks. In particular, it highlights that agentic components are different from simple LLM-based applications and necessitate additional controls throughout the entire lifecycle. In particular, it recommends the following.

- Pre-deployment, test agents for safety and security, eg, test for new dimensions such as overall task execution and tool use accuracy and test at

different levels across varied datasets to capture the full spectrum of agent behaviour.

- When deploying, gradually roll out agents and continuously monitor them in production.

### 6.3 Cybersecurity in the Healthcare Sector

While there are no specific cybersecurity obligations pertaining to the healthcare sector, the healthcare sector has been gazetted as one of 11 sectors providing essential services. As such, designated owners of CII (and other designated entities under the Cybersecurity Act) within the healthcare sector are subject to the same requirements as laid out in **2.2 Critical Infrastructure Cybersecurity Requirements**.

Where applicable, healthcare providers must also comply with the National Telemedicine Guidelines, which include data protection and security requirements. In so far as a medical device is used by an organisation to collect personal data (eg, device test results are uploaded onto a server owned by the organisation), the organisation must comply with the protection obligation under the PDPA (as described in **6.1 Cybersecurity and Data Protection**).

The Cyber and Data Security Guidelines for Healthcare Providers (the “Healthcare Guidelines”) provide guidance on the cyber and data security measures to be put in place for the proper storage, access, use and sharing of health information to improve the security posture among healthcare providers. Healthcare providers can also refer to the Cyber and Data Security Guidebook for healthcare providers for explanations and references to resources from the CSA and the PDPC. While not mandatory, the requirements within the Healthcare Guidelines will eventually be imposed as regulatory requirements under the forthcoming Health Information Act.

In October 2024, the Cybersecurity Labelling Scheme for Medical Devices (CLSMD), jointly developed by the CSA, the Ministry of Health, the Health Sciences Authority and Synapse, was launched. Under this voluntary scheme, medical devices are rated according to four levels of cybersecurity provisions. The label aims to improve security awareness by making the cybersecurity provisions of medical devices more transparent. The CLSMD applies to medical devices

as described in the First Schedule of the Health Products Act 2007.

At the time of writing, Singapore's parliament is also debating the Health Information Bill, which will establish a dedicated statutory framework for contributing to and accessing the National Electronic Health Record system, as well as for wider health information sharing and protection. Under the Health Information Bill, healthcare providers are required to report a confirmed cybersecurity incident or data breach to the Ministry of Health, with an initial report required within two hours and a detailed incident report required within 14 days. This framework also includes cybersecurity and data security requirements for healthcare providers and other persons who contribute to or access the National Electronic Health Record system.

---

## CHAMBERS GLOBAL PRACTICE GUIDES

---

Chambers Global Practice Guides bring you up-to-date, expert legal commentary on the main practice areas from around the globe. Focusing on the practical legal issues affecting businesses, the guides enable readers to compare legislation and procedure and read trend forecasts from legal experts from across key jurisdictions.

To find out more information about how we select contributors, email [Rob.Thomson@chambers.com](mailto:Rob.Thomson@chambers.com)