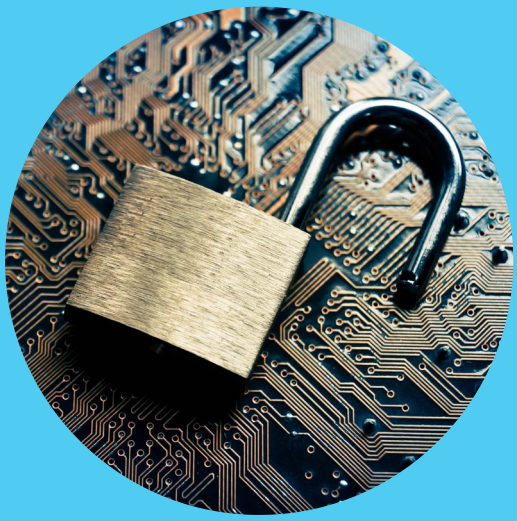
STEPHENSON HARWOOD



A guide to cybersecurity: what you need to know

Contents

Cybersecurity refers to the need to protect the following from unlawful use, access or interference:

- **Information and data stored electronically (rather than in physical form).**
- **The communications network which underpins modern society and business and government functions.**

Why do you need to protect your organisation from cyber-attacks?

Cybersecurity threats have increased due to the far greater use of digital technologies. A cyber-attack can result in:

- Contractual/tortious liability towards individuals seeking compensation for damage and/or distress caused by unlawful acquisition, disclosure and/or use of personal information.
- Prosecution/regulatory sanction by failing to comply with legal obligations to keep information and networks secure or, in some cases, failing to respond appropriately in the event of a cyberattack.
- Reputational damage.

How can organisations manage the risks posed by cyber-attacks?

Every organisation will have to consider how much time and money to spend on protecting their technology and services from cyber-attacks. Regulatory bodies have advised against carrying out cyber risk management for "compliance" only as this can lead to risks being managed in a "tick-box" fashion which ignores the fact that all organisations will be operating under different levels of risk and therefore require different approaches to risk management.

When considering cybersecurity obligations, organisations should include managing risk within its supply chain and outsourcing to service providers. Risks can be managed by implementing various technical and organisational precautions and procedures, inserting appropriate provisions into commercial contracts, obtaining adequate insurance, identifying applicable laws and regulations and ensuring compliance.

Organisations should ensure they have a cyber-breach response plan, which should take into account the relevant notification obligations which apply under applicable cybersecurity laws.

This note sets out some of the key obligations and practical steps organisations must consider across different jurisdictions in order to meet their cybersecurity obligations.

UK/EU

Key obligations

All business that collect or process personal data of individuals must implement appropriate technical and organisational measures to ensure a level of security appropriate to risk under the GDPR.

Any operator of essential services in the key sectors of energy, transport, banking, financial market infrastructures, health sector, water supply and distribution and digital infrastructure, and certain "digital service providers" (providers of information society services of the following types: online marketplaces, search engines and cloud computing services) must to take appropriate proportional technical and organisational measures to manage risks to networks and information systems and take appropriate measures to minimise the impact of incidents under the Network and Information Security Directive.

If you provide a public electronic communications network or service or carry out marketing by phone, email, text or fax; use cookies or similar technology on your website; or compile a telephone directory, you must take appropriate technical and organisational measures to safeguard the security of that service under the Privacy and Electronic Communications Regulations.


11:45
Monday
538.19
11:45 AM
STOCK EXCHANGE

Enforcement examples

DSG Retail Limited experienced a cyber-attack in which malware had been installed and was running on over 5,000 point of sale terminals which enabled the attacker to collect payment card details for any transactions using those terminals between July 2017 and April 2018. They were fined £500,000 by the ICO for failure to implement appropriate computer systems and organisational measures. Failures included:

- insufficient network segregation
- no local firewall configured on the terminals
- inadequate approach to software patching of its domain controllers
- failure to run regular vulnerability scanning to assess threat level
- inconsistent whitelisting processes for the terminals (i.e. explicitly allowing some identified entities access to a particular privilege and blocking others)
- failure to implement system of logging and monitoring incidents in order to respond in a timely manner
- outdated software
- lack of point to point encryption failure to carry out adequate risk assessments
- failure to implement standard builds based on industry standard hardening guidance.

The ICO found these contraventions to be serious.

Cathay Pacific Airways Limited was fined £500,000 for failing to protect the security of its customers' personal data. The ICO found the following deficiencies it the company's data security:

- database backups which were not encrypted
- the internet-facing server was accessible due to a known and publicised vulnerability
- the administrator console was publically accessible via the internet
- the use of operating systems which were no longer supported by necessary security updates
- failure to remove any unnecessary applications, features, services and ports to minimise attack points
- network users were permitted to authenticate past the VPN without multi-factor authentication
- inadequate anti-virus protection
- inadequate patch management (i.e. scanning machines on the network for missing software updates)
- failure to preserve digital evidence to assist the ICO's investigation
- inappropriate privileges given to some user accounts
- inadequate penetration testing to assess threat level of cyber-attack
- data retained for too long.

The ICO deemed this lack of protective security measures and policies in place as particularly serious given the quantity and nature of the data controlled and processed which included passport numbers, contact details and dates of birth.

UAE

Key obligations

From 1 July 2020, all businesses operating, conducting or attempting to conduct business in or from the DIFC must implement appropriate technical and organizational measures to protect personal data against wilful, negligent, accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access under the DIFC Data Protection Law 2020.

All Abu Dhabi Global Market ("ADGM") registered entities that collect or process personal information must implement appropriate technical and organisational measures to protect data against unlawful or unauthorised processing and accidental loss, destruction or damage under the ADGM Data Protection Regulations 2015.

All licensed healthcare professionals, alternative medicine professionals and healthcare operators ("Licensees") must treat security as an essential element of their information systems and networks. Licensees that hold patient health information have additional obligations under the DHCC Health Data Protection Regulations.

Please note the above are some of the key legislations in the UAE however there is no standalone information security law applicable throughout the UAE. The UAE applies security and privacy laws to specific sectors and business transactions including healthcare, telecommunications, e-commerce, electronic payments.

The UAE's Cyber Crime Law (Federal Law No.5 of 2012) imposes significant penalties and punishments for those committing cybercrime. The Cyber Crime Law focusses on protecting internet users from violation of their privacy relating to information published online and criminalising various online activities.

Hong Kong

Key obligations

All businesses that collect or process the personal data of individuals must take all practical steps to ensure that any personal data held by businesses is protected against unauthorized or accidental access, processing, erasure, loss or use under the Personal Data (Privacy) Ordinance ("PDPO").

Regulatory bodies in certain sectors have issued sector-specific non-binding guidelines in relation to cybersecurity. The guidelines do not contain strict legal obligations however they do contain highly persuasive advice on certain cybersecurity standards for the relevant sectors such as responsibilities of personnel and directors in relation to overseeing and implementing cybersecurity measures and the minimum protective measures required within that sector (including two-factor authentication log-ins, surveillance for unauthorised access, encryption and multi-tiered firewalls).

Please note there is no dedicated statute in Hong Kong that specifically addresses cybersecurity. The PDPO is relevant if personal data privacy issues are concerned.

Enforcement example

Cathay Pacific Airways (and its affiliate Hong Kong Dragon Airlines) received an enforcement notice from the PCPD on 6 June 2019 in respect of a data breach concerning unauthorised access to the personal data of around 9.4 million Cathay Pacific customers. This was the same incident which resulted in the penalty notice from the ICO above. The enforcement notice concerned breach of Data Protection Principle 4 "to take all practicable steps to ensure that personal data are protected against unauthorised access" and a breach of certain retention obligations under the PDPO. Some key practical compliance points from the enforcement notice included:

- the failure of the organisation to implement sufficient vulnerability scanning of an internet-facing server
- no requirement across the business to use multi-factor authentication
- failure to assemble a personal data inventory
- deficient controls on restricting external access to the administrator console
- failure to encrypt database backup files.

The enforcement notice provided a list of recommendations for Cathay Pacific to follow to resolve the issue including engaging an independent data security expert to overhaul the system, implement multi-factor authentication and carry out regular vulnerability screenings.

PRC

Key obligations

All network operators, "critical information infrastructure operators" ("CIIO") and providers of network products and services must implement technical and other necessary measures to ensure the security of personal information and to prevent the data from being actively disclosed, tampered with or destroyed under the Cybersecurity Law 2017 ("CSL 2017"). Network operators must also provide technical support and assistance to law enforcement authorities to safeguard national security and investigate crimes. CIIOs must also sign security and confidentiality agreements with their suppliers of network products and services, and evaluate cybersecurity and other potential risks at least once a year under the CSL 2017.

All internet service providers and other enterprises that collect or use citizens' personal electronic information in the course of their business must take technical measures and other necessary measures to ensure information security and prevent the leakage, damage and loss of personal electronic information of citizens collected in business activities under the Decision of the Standing Committee of the National People's Congress on Strengthening Network Information Protection ("2012 Decision").

All network operators as defined in the CSL 2017 must comply with the national security standards as set out in Muti-level Protection Scheme 2.0 (MLPS 2.0). Network operators must classify their network and information systems into different levels and implement security protections accordingly in order to safeguard national cyberspace, ensure public interest and protect the rights and interests of citizens and legal persons under the MPLS 2.0.

Please note the CSL 2017 is China's first comprehensive privacy and security regulation for cyberspace. As the CSL 2017 is a high-level law and does not provide practical guidelines, China has been and it still in the process of drafting a series of related implementation rules and guidelines which should be followed to ensure best practice.

Enforcement examples

A Shantou technology company was penalised in July 2017 for violating the CSL 2017 and the Administrative Measures for Tiered Protection of Information Security (a non-binding guideline) on the grounds that the company did not fulfil its obligations to conduct security evaluations for its information systems. The internet police ordered the company to implement corrective action to remedy the offence.

A website for teacher training and education was penalised in 2017 for failing to implement the CSL 2017's tiered system of cybersecurity protections and security assessment which resulted in serious cybersecurity shortcomings and led to network intrusion incidents. The company was fined 10,000 yuan (~$1,500) and the managerial officer was personally fined 5,000 yuan (~750,000) under the CSL 2017.

Seven telecommunications companies were penalised in November 2018 for failing to fulfil their obligations under the CSL 2017 and certain sectoral regulations. These included failure to file for an MLPS classification, failure to establish internal policies and procedures for the collection and use of personal information and failing to launch the security assessment process for new services.

Future developments

It should be noted that the Legal Committee of the National People's Congress Standing Committee announced in late December 2019 that the enactment of legislation on personal data protection and security is a priority in the next legislative year. As such, it is recommended that organisations continue to monitor the developments of the PRC data protection and cyber security regulatory regime.

Singapore

Key obligations

Public and private owners of a critical information infrastructure ("CII") are subject to the codes and directions issued by the Commissioner of Cybersecurity. CIIs are also required to conduct regular audits and risk assessments for cybersecurity vulnerabilities. Cybersecurity service providers (managed security operations centre monitoring services and penetration testing services) must be deemed "fit and proper" by the licensing officer under the Cybersecurity Act 2018 (No.9 of 2018).

All organisations that collect or process the personal data of individuals must implement policies and practices that comply with the obligations set out in the Personal Data Protection Act 2012 (No. 26 of 2012), as further supplemented by the guidelines provided by the Personal Data Protection Commission.

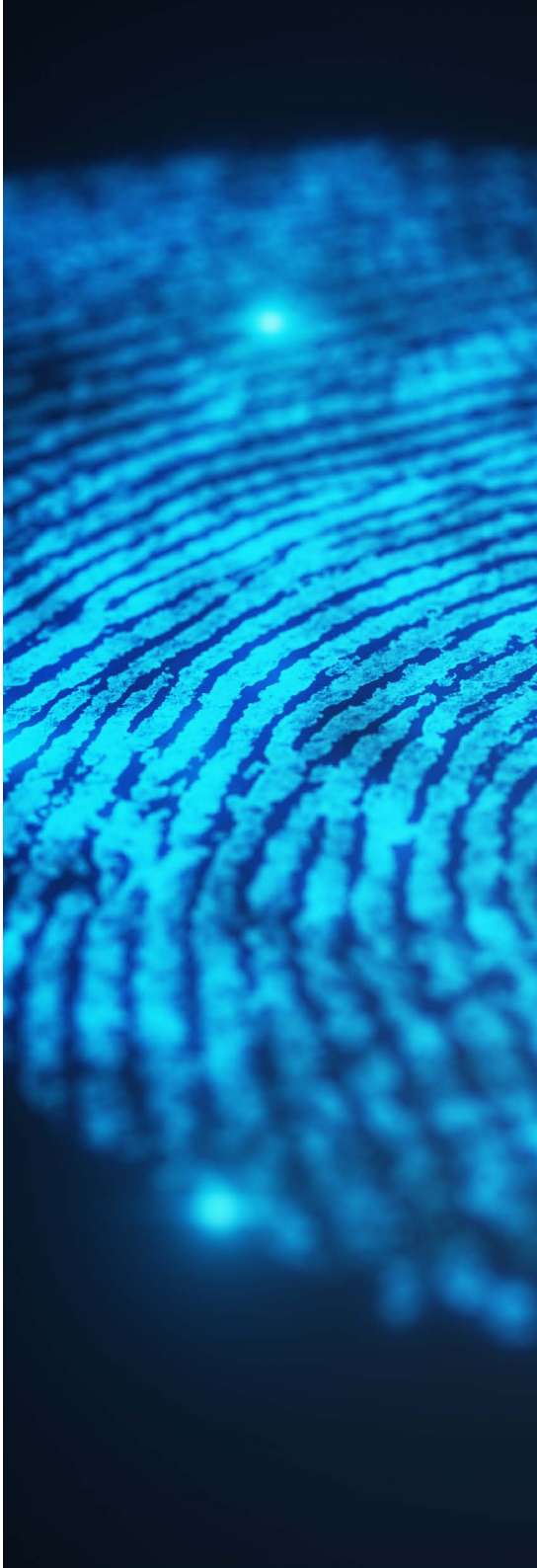
All network-connected consumer smart devices and consumer Internet of Things (i.e. WiFi routers and smart home hubs) may wish to: implement basic security requirements; adhering to principles of Security-by-Design; ensuring an absence of common software vulnerabilities; and ensuring resistance to basic penetration testing under the voluntary Cybersecurity Labelling Scheme.

Enforcement example

SingHealth and its IT vendor, IHiS, had failed to put in place reasonable security measures to protect patients' data. Both were therefore liable for breaching the Protection Obligation under the Personal Data Protection Act. As a result, SingHealth was fined a hefty S$250,000, while IHiS was fined an even heftier S$750,000. This case emphasises that organisations have a primary role and responsibility of ensuring the overall protection of the personal data in its possession or control, even if they engage a data intermediary.

A practical checklist

- Keep software up to date.
- Keep malware protection up to date.
- Implement firewalls to cover entire IT networks as well as individual devices which can block downloads, access to malicious domains and prevent users' computers from communicating directly with the internet.
- Implement sufficient patch management procedures to patch known vulnerabilities with the latest version of software to prevent attacks which exploit software bugs.
- Ensure password policies are in place and followed. All passwords should be secure and include a combination of lowercase, uppercase, letters, numbers and symbols.
- Restrict IT admin and access rights to specific users.
- Back up data securely via a cloud service.
- Implement rules and policies for storing and moving personal data securely.
- Train staff and raise awareness of cyber-attacks and the potential signs of a threat.
- Use full disc encryption and/or file encryption to secure data.
- Establish an incident response and disaster recovery process to ensure compliance with notification obligations.



Why Stephenson Harwood LLP?

Stephenson Harwood is a law firm with over 1300 people worldwide, including more than 190 partners. Our people are committed to achieving the goals of our clients – listed and private companies, institutions and individuals.

We assemble teams of bright thinkers to match our clients' needs and give the right advice from the right person at the right time. Dedicating the highest calibre of legal talent to overcome the most complex issues, we deliver pragmatic, expert advice that is set squarely in the real world.

Our headquarters are in London, with eight offices across Asia, Europe and the Middle East. In addition we have forged close ties with other high quality law firms and an integrated local law capability in Singapore and the PRC. This diverse mix of expertise and culture results in a combination of deep local insight and the capability to provide a seamless international service.

GET IN TOUCH

UK, EU

Simon Bollans
Partner
T: +44 20 7809 2668
E: simon.bollans@shlegal.com

Michael Bywell
Partner
T: +44 20 7809 2765
E: michael.bywell@shlegal.com

Peter Dalton
Partner
T: +44 20 7809 2151
E: peter.dalton@shlegal.com

Katie Hewson
Partner
T: +44 20 7809 2374
E: katie.hewson@shlegal.com

Dubai

Kiersten Lucas
Partner
T: +971 4 407 3993
E: kiersten.lucas@shlegal.com

Emily Aryeetey
Senior associate
T: +971 4407 3942
E: emily.aryeetey@shlegal.com

Singapore

Sheetal Sandhu
Partner, Stephenson Harwood (Singapore) Alliance*
T: +65 6661 6523
E: sheetal.sandhu@shlegalworld.com

Hong Kong

Katherine Liu
Partner
T: +852 2533 2717
E: katherine.liu@shlegal.com

Mark Reed
Partner
T: +852 2533 2888
E: mark.reed@shlegal.com

Guangzhou

Zoe Zhou
Partner, Stephenson Harwood – Wei Tu (China) association**
T: +86 20 8388 0590
E: zoe.zhou@shlegalworld.com

www.shlegal.com

STEPHENSON HARWOOD

BD1037-A guide to cybersecurity-0323