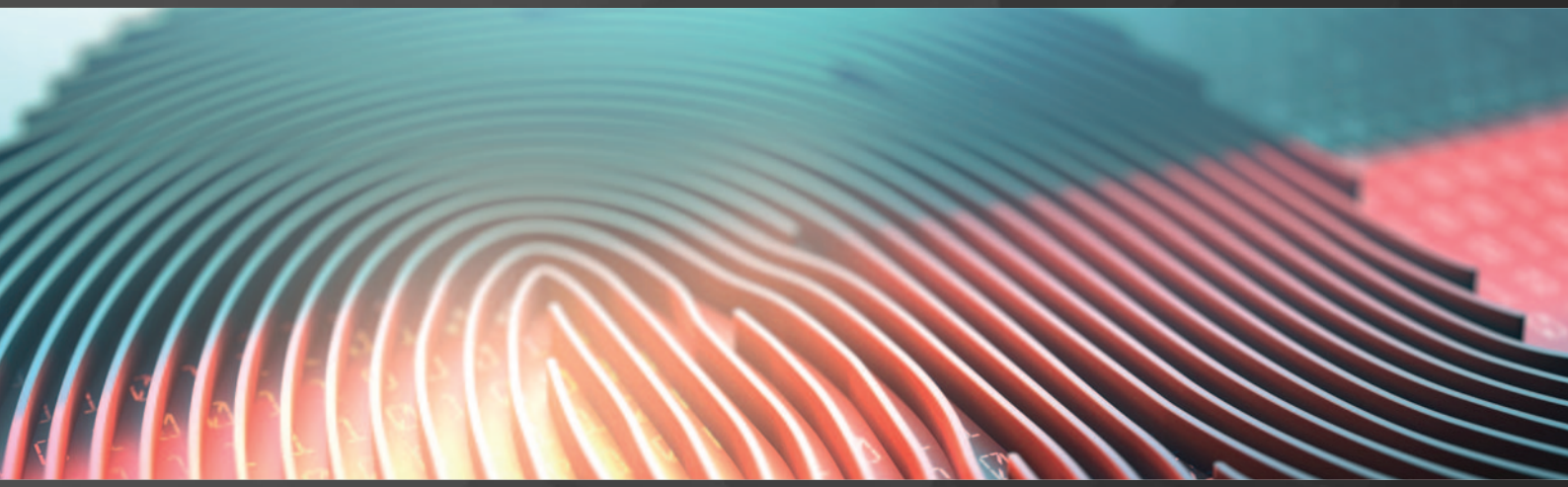
International Comparative Legal Guides



Cybersecurity 2020

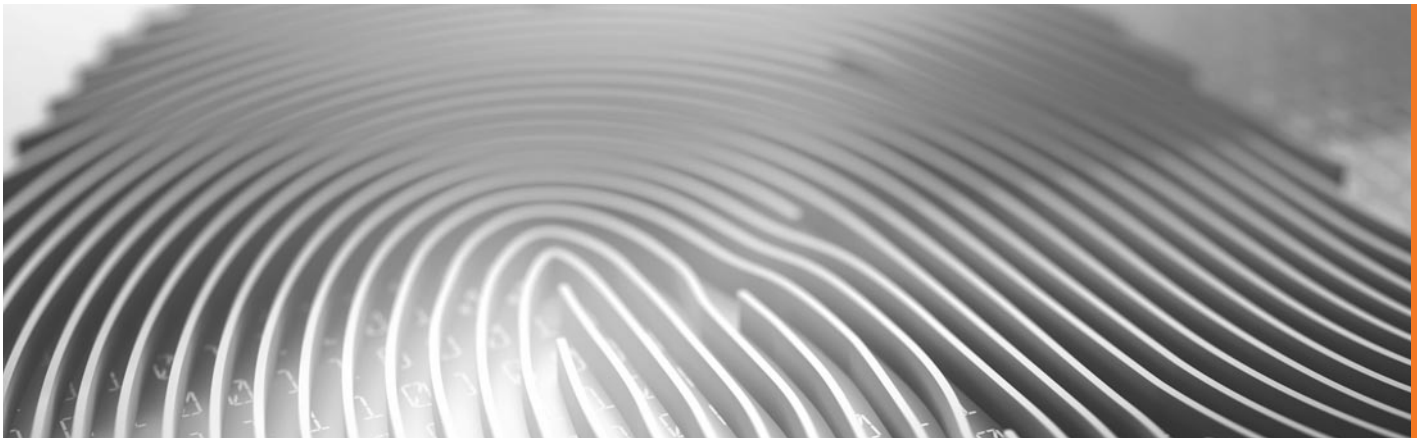
A practical cross-border insight into cybersecurity law

Third Edition

Featuring contributions from:

Advokatfirmaet Thommessen AS
Allen & Overy LLP
Boga & Associates
Christopher & Lee Ong
Cliffe Dekker Hofmeyr
Creel, García-Cuéllar, Aiza y Enríquez, S.C.
Eversheds Sutherland
Faegre Baker Daniels
G+P Law Firm
Gikera & Vadgama Advocates
Gouveia Pereira, Costa Freitas & Associados, Sociedade de Advogados, S.P., R.L.
Iwata Godo
King & Wood Mallesons
Lee & Ko
Lee and Li, Attorneys-at-Law
LEĜA
Lesniewski Borkiewicz & Partners (LB&P)
Maples Group
McMillan
Mori Hamada & Matsumoto
Niederer Kraft Frey Ltd.
Nyman Gibson Miralis
Pearl Cohen Zedek Latzer Baratz
R&T Asia (Thailand) Limited
Rajah & Tann Singapore LLP
Ropes & Gray
SAMANIEGO LAW
Shardul Amarchand Mangaldas & Co.
Siqueira Castro – Advogados
Sirius Legal
Stehlin & Associés
Synch

ICLG.com



ISBN 978-1-83918-005-7
ISSN 2515-4206

Published by
global legal group
59 Tanner Street
London SE1 3PL
United Kingdom
+44 207 367 0720
www.iclg.com

Group Publisher
Rory Smith

Associate Publisher
James Strode

Senior Editors
Caroline Oakley
Rachel Williams

Deputy Editor
Hollie Parker

Creative Director
Fraser Allan

Printed by
Stephens & George
Print Group

Cover Image
www.istockphoto.com

Cybersecurity 2020

Third Edition

Contributing Editors:
Nigel Parker and Alexandra Rendell
Allen & Overy LLP

Strategic Partners

Expert Chapters

Country Q&A Chapters

ICLG.com

From the Publisher

Dear Reader,

Welcome to the third edition of *The International Comparative Legal Guide to Cybersecurity*, published by Global Legal Group.

This publication, which is also available at www.iclg.com, provides corporate counsel and international practitioners with comprehensive jurisdiction-by-jurisdiction guidance to cybersecurity laws and regulations around the world.

This year, there are three general chapters which provide an overview of key issues affecting cybersecurity, particularly from the perspective of a multi-jurisdictional transaction.

The question and answer chapters, which cover 32 jurisdictions in this edition, provide detailed answers to common questions raised by professionals dealing with cybersecurity laws and regulations.

As always, this publication has been written by leading cybersecurity lawyers and industry specialists, to whom the editors and publishers are extremely grateful for their invaluable contributions.

Global Legal Group would also like to extend special thanks to contributing editors Nigel Parker and Alexandra Rendell of Allen & Overy LLP for their leadership, support and expertise in bringing this project to fruition.

Rory Smith
Group Publisher
Global Legal Group

Israel

Pearl Cohen Zedek Latzer Baratz

Haim Ravia

Dotan Hammer

1 Criminal Activity

1.1 Would any of the following activities constitute a criminal offence in your jurisdiction? If so, please provide details of the offence, the maximum penalties available, and any examples of prosecutions in your jurisdiction:

Hacking (i.e. unauthorised access)
Section 4 of the Israeli Computers Law, 5755-1995 criminalises unlawful intrusion into computer material. The term "intrusion into computerized material" is defined in the statute as "intrusion by communicating with or connecting to a computer, or by operating it, but excluding intrusion that constitutes wiretapping" under the Israeli Wiretap Law, 5739-1979. This offence carries a maximum penalty of three years' imprisonment.

Section 5 of the Computers Law penalises intrusion into computer material committed in furtherance of another predicate felony. The maximum penalty for this offence is five years' imprisonment.

A 2017 landmark Supreme Court judgment broadly interpreted the boundaries of the term "intrusion into computerized material" to cover any access to a computer absent of the owner's permission or some other legal authority. Prosecutions of this offence are becoming more abundant, such as with disgruntled former employees hacking into their former employer's systems, hackers hacking into web-connected cameras, terrorism-oriented hacking and bank account hacking.

Denial-of-service attacks
Denial of service attacks fall within the scope of Section 2 of the Israeli Computers Law, which penalises any obstructions to the ordinary operation of a computer or interference with its use. The maximum penalty for this offence is three years' imprisonment.

Phishing
Phishing falls within the scope of two traditional offences codified in the Israeli Penal Law, 5737-1977, the first being receipt of something by fraud (Section 415 of the Penal Law). This offence is punishable by a maximum term of three years in prison, but if the offence is committed in aggravating circumstances, the maximum punishment is five years in prison. The second offence is receipt of something by ploy or by intentional exploitation of another person's mistake (Section 416 of the Penal Law), punishable by two years' imprisonment. These offences have been the subject of indictments such as online bank account phishing and Facebook account phishing.

Infection of IT systems with malware (including ransomware, spyware, worms, trojans and viruses)
Section 6 of the Israeli Computers Law criminalises the programming or adaptation of a computer program for the purpose of unlawfully performing any one of six enumerated acts. Among the enumerated acts is interfering with the ordinary operation of a computer, impacting the integrity of computerised content, facilitating unlawful intrusion into computers or invading a person's privacy. This offence is punishable by up to three years' imprisonment. The act of trafficking in or installing such computer programs is punishable by up to five years in prison. Developers and distributers of spyware, worms, trojans and viruses have been prosecuted under these provisions.

Possession or use of hardware, software or other tools used to commit cybercrime (e.g. hacking tools)
The installation of software or other tools used to commit cybercrime is an offence under Section 6 of the Israeli Computers Law. This also applies to hardware with a firmware component. While mere possession is likely not an offence, it may amount to an attempt to commit the offence. An attempt is punishable by the same prison term prescribed for the completed offence.

Identity theft or identity fraud (e.g. in connection with access devices)
Identity theft or identity fraud can give rise to two traditional offences codified in the Israeli Penal Law, 5737-1977 – receipt of something by fraud and receipt of something by ploy, both discussed above. In addition, using the identity credentials of another person can give rise to the offence of impersonating another person with intent to defraud, codified in Section 441 of the Israeli Penal Law and punishable by up to three years in prison.

Electronic theft (e.g. breach of confidence by a current or former employee, or criminal copyright infringement)
Electronic theft can give rise to the traditional offence of larceny codified in the Israeli Penal Law, punishable by up to three years in prison, or up to seven years if the stolen property is valued at ILS 500,000 or more. Theft by an employee is a more egregious offence, punishable by up to seven years' imprisonment. If the theft involves data whose confidentiality was compromised by the theft, and the confidentiality arises from an obligation under law, the theft amounts to a criminal invasion of privacy punishable by up to five years' imprisonment.

Copying, importing, renting out or distributing infringing copies of copyrighted material, as well as possession of such copies for the purpose of trafficking are offences under the Israeli Copyright Law, 5768-2007 if they are committed in a commercial scope. These are punishable by up to five years' imprisonment.

Any other activity that adversely affects or threatens the security, confidentiality, integrity or availability of any IT system, infrastructure, communications network, device or data

Other activities that adversely affect or threaten the security, confidentiality, integrity or availability of any IT system, infrastructure, communications network, device or data are likely captured by the above offences.

Failure by an organisation to implement cybersecurity measures

Under the Israeli Protection of Privacy Law, 5741-1981, certain organisations are required to appoint an information security officer. Details can be found in the answer to question 4.2 below. Under Section 31A(a)(6) of the Israeli Protection of Privacy Law, failure to appoint an information security officer where such is mandated by the law is a strict lability offence punishable by up to one year in prison.

1.2 Do any of the above-mentioned offences have extraterritorial application?

The above offences have extraterritorial application in three main scenarios. First, if the offence was only partially committed outside Israel, the conduct will be fully captured by the above offences.

Second, if preparations to commit the offence, an attempt to commit it, inducement of another to commit the offence, or conspiracy to commit the offence were performed outside Israel, but the completed offence would have been committed in whole or in part in Israel, then the conduct will be fully captured by the above offences.

Finally, where an offence was committed outside Israel but was targeted against the State of Israel in the broad sense of the phrase (e.g., against national security, the State's regime, the State's property or economy), or was committed by an Israeli resident or citizen, then the conduct will be fully captured by the above offences.

1.3 Are there any actions (e.g. notification) that might mitigate any penalty or otherwise constitute an exception to any of the above-mentioned offences?

The traditional affirmative defences to criminal culpability also apply to these offences. These defences include necessity, duress and self-defence, yet the bar is rather high to meet. Additionally, both prosecutorial discretion and sentencing guidelines would take into account mitigating factors such as the severity of the conduct, the degree of wilfulness, the scope of harm or affected victims, the motives, etc.

1.4 Are there any other criminal offences (not specific to cybersecurity) in your jurisdiction that may arise in relation to cybersecurity or the occurrence of an Incident (e.g. terrorism offences)? Please cite any specific examples of prosecutions of these offences in a cybersecurity context.

Several other criminal offences which in themselves are not specific to cybersecurity have been used to indict defendants in Israel. Under the specific circumstances of those cases, those charges were applied to cybersecurity matters or to Incidents.

In a recent case, the State of Israel indicted a former employee of an Israeli cyber company in the cyber intelligence business. The defendant was charged with misappropriating intellectual property (cyber and espionage software) and attempting to sell it for $50 million over the Darknet, in a manner potentially harmful to national security. He was also indicted for an attempt to damage property aimed at impairing national security, an offence under section 108 of the Penal Law, and for marketing export-controlled materials without a defence marketing licence, an offence under section 32 of the Defense Export Control Law, 5767-2007.

In the criminal case of *Israel v. Abu Atza*, the defendant was accused of breaking into a victim's car and stealing her handbag, which contained her smartphone. He allegedly published intimate photos of her which he found on her phone, posting them on her own Instagram account. He was also indicted for sexual harassment, an offence under section 3 of the Prevention of Sexual Harassment Law, 5758-1998.

In the case of *Israel v. Oyda*, the defendant, a resident of the Gaza Strip, used software named "Website Hacking" to access the Israeli Police's website and display live streams of traffic cameras in order to gather intelligence against the State of Israel. The defendant had also accessed drone telecommunications for these purposes. He was also indicted with and convicted of membership and activity in an illegal organisation, an offence under section 85 of the Defense Regulations, and espionage, an offence under section 112 of the Penal Law.

In the case of *Israel v. Massrawa*, the defendant used usernames and passwords he collected through a phishing scam, in order to access victim's bank accounts and transfer funds from those accounts. He was also indicted with and convicted of money laundering, an offence under section 3 of the Prohibition on Money Laundering Law, 5760-2000.

In the case of *Israel v. Mualem* (decided on June 30, 2016), the defendant installed monitoring software called "SpyPhone" on personal phones of victims, at the requests of private investigators. The defendant was charged with and convicted of assisting wiretapping without proper authority, an offence under section 2 of the Wiretap Law.

2 Applicable Laws

2.1 Please cite any Applicable Laws in your jurisdiction applicable to cybersecurity, including laws applicable to the monitoring, detection, prevention, mitigation and management of Incidents. This may include, for example, laws of data protection, intellectual property, breach of confidence, privacy of electronic communications, information security, and import/export controls, among others.

Laws applicable to cybersecurity include the Israeli Computers Law, the Protection of Privacy Law, the Penal Law, the Defense Export Control Law, the Regulation of Security in Public Bodies Law, and the recently proposed Cyber Defense and National Cyber Directorate Bill.

2.2 Are there any cybersecurity requirements under Applicable Laws applicable to critical infrastructure in your jurisdiction? For EU countries only, please include details of implementing legislation for the Network and Information Systems Directive and any instances where the implementing legislation in your jurisdiction exceeds the requirements of the Directive.

The Regulation of Security in Public Bodies Law authorises the Israeli Security Agency and the National Cyber-defense Authority to issue binding directives to organisations operating critical infra-

structures on matters related to information security and cybersecurity, and inspect such organisations' compliance with those directives. Organisations subject to this regime include telecom and internet providers, transportation carriers, the Tel Aviv Stock Exchange, the Israeli Internet Association, utility companies and others.

2.3 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to take measures to monitor, detect, prevent or mitigate Incidents? If so, please describe what measures are required to be taken.

Aside from the cybersecurity requirements applicable to critical infrastructures as explained in the preceding question, the Protection of Privacy Regulations (Data Security), 5777-2017, is an omnibus set of rules. It requires any Israeli organisation that owns, manages or maintains a database containing personal data to implement prescriptive security measures, whose main objective is the prevention of Incidents. These include, for example, physical security measures, access control measures, risk assessment and penetration tests. The regulations classify databases into four categories (basic, intermediate, high and those held by individuals), with each subject to an escalating set of information security requirements.

The regulations also require organisations to monitor and document any event that raises suspicion of compromised data integrity or unauthorised use of data.

Additionally, organisations that hold certain sensitive information are required under the data security regulations to implement an automated audit mechanism to monitor any attempt to access information systems that contain personal data. Sensitive information covers information regarding an individual's private affairs, including: individuals' behaviour in the private domain; health or mental condition; political opinions or religious beliefs; criminal history; telecommunication meta data; biometric data; financial information regarding individuals' assets, debts and economic liabilities; and consumption habits of an individual which may be indicative of the above-mentioned types of data.

In addition, financial institutions and insurance companies are required to operate a security operation centre tasked with monitoring, detecting and mitigating cybersecurity risks.

2.4 In relation to any requirements identified in question 2.3 above, might any conflict of laws issues arise? For example, conflicts with laws relating to the unauthorised interception of electronic communications or import/export controls of encryption software and hardware.

Use of certain information security measures may constitute telecommunication wiretapping or invasion of privacy. The Israeli Protection of Privacy Law prescribes a number of affirmative defences to invasion of privacy, which are arguably invokable in case of a conflicting legal requirement. Additionally, Section 64 of the proposed Cyber Defense and National Cyber Directorate Bill proposes an exemption from liability for unlawful wiretapping, invasion of privacy, or intrusion into computers, if an organisation takes steps in furtherance of cybersecurity, maintains a cybersecurity policy and is transparent to affected individuals about its use of cybersecurity measures.

2.5 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents (including cyber threat information, such as malware signatures, network vulnerabilities and other technical characteristics identifying a cyber attack or attack methodology) to a regulatory or other authority in your jurisdiction? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; (b) the regulatory or other authority to which the information is required to be reported; (c) the nature and scope of information that is required to be reported; and (d) whether any defences or exemptions exist by which the organisation might prevent publication of that information.

There are several provisions according to which certain organisations are required to report Incidents.

First, under the Israeli data security regulations, any organisation that is subject to the intermediate security level or the high security level is required to notify the Protection of Privacy Authority (the Israeli privacy regulator) of the Incident. The notification must state the measures taken to mitigate the Incident. The Protection of Privacy Authority is vested with investigative powers and can request and obtain additional information accessible to the organisation about the Incident, including malware signatures, network vulnerabilities and other technical characteristics identifying a cyber-attack or attack methodology.

The intermediate security level applies to public agencies, organisations that hold sensitive information and data brokers. The high security level applies to organisations that hold sensitive information or data brokers, in each case of at least 100,000 data subjects or with more than 100 persons with access credentials.

Second, financial institutions and insurance companies are required to report Incidents pursuant to regulatory guidelines by the Israeli Banking Regulator, and insurance companies are required to report to the Israel's Capital Market, Insurance and Savings Authority within the Ministry of Finance.

Third, under the Cyber Defense and National Cyber Organization Bill, the National Cyber Organization and the Israeli Security Agency (colloquially known as the Shin Bet) can approach any organisation in Israel and demand any document and information it has relating to an Incident, instruct the organisation on how to operate its IT system and seize computers, communication systems and drives containing data.

There are no formally specified defences or exemptions by which an organisation might prevent publication of information relating to an Incident.

2.6 If not a requirement, are organisations permitted by Applicable Laws to voluntarily share information related to Incidents or potential Incidents (including cyber threat information, such as malware signatures, network vulnerabilities and other technical characteristics identifying a cyber attack or attack methodology) with: (a) a regulatory or other authority in your jurisdiction; (b) a regulatory or other authority outside your jurisdiction; or (c) other private sector organisations or trade associations in or outside your jurisdiction?

Voluntarily sharing information about an Incident with the Israeli privacy regulator is a permissible practice that the Israeli privacy regulator encourages in the present cybersecurity landscape. If the Incident eventually turns out to be one for which a notification to the regulator was required, the Israeli privacy regulator will tend to view the voluntary early disclosure as a mitigating factor in regulatory action it might take.

Sharing information about an Incident with a foreign authority is the *de facto* result of non-Israeli data breach notification laws with a long reach, such as the GDPR and state data breach notification laws in the United States.

Finally, sharing information about an Incident with other private sector organisations or trade associations in Israel raises anti-trust issues, but is conditionally permissible pursuant to the Anti-Trust Commissioner's opinion from 2017, if the information shared does not pertain to the business activities of the organisation.

2.7 Are organisations required under Applicable Laws, or otherwise expected by a regulatory or other authority, to report information related to Incidents or potential Incidents to any affected individuals? If so, please provide details of: (a) the circumstance in which this reporting obligation is triggered; and (b) the nature and scope of information that is required to be reported.

In certain circumstances, the Israeli privacy regulator may order the organisation after consultation with the Head of the National Cybersecurity Authority, to report the Incident to all affected data subjects. No test case has triggered this to date and thus the particulars of this issue are not yet known.

2.8 Do the responses to questions 2.5 to 2.7 change if the information includes: (a) price-sensitive information; (b) IP addresses; (c) email addresses (e.g. an email address from which a phishing email originates); (d) personally identifiable information of cyber threat actors; and (e) personally identifiable information of individuals who have been inadvertently involved in an Incident?

The data breach notification obligation, as applied by the Israeli data security regulations, depends on the database's security level, which in turn depends on the nature of the information it stores. See the answer to question 2.5 for more information. Yet if the breached data is not capable of identifying an individual, then the Incident need not be reported, since it does not pertain to regulated "personal data".

2.9 Please provide details of the regulator(s) responsible for enforcing the requirements identified under questions 2.3 to 2.7.

The Israeli privacy regulator is responsible for enforcing the data security regulations. The Banking Supervisor at the Bank of Israel is responsible for enforcing the data breach rules relating to Incidents in banks and credit card companies. The Supervisor of Capital Markets, Insurance and Savings within the Israeli Ministry of Finance is responsible for enforcing the data breach rules relating to Incidents at insurance companies.

2.10 What are the penalties for not complying with the requirements identified under questions 2.3 to 2.8?

There are currently no penalties imposable by the Israeli privacy regulator for failing to comply with the data breach notification requirement. A proposed amendment to the Israeli Protection of Privacy Law would empower the regulator with authority to impose penalties.

2.11 Please cite any specific examples of enforcement action taken in cases of non-compliance with the above-mentioned requirements.

In 2017, the Israeli privacy regulator investigated a data breach revealed in an Israeli company in the business of vehicle location monitoring. The data breach was revealed by an anonymous hacker, who exploited a security vulnerability in the company's website. The regulator launched enforcement action against the company and concluded that it had violated the Israeli data security regulations by not providing a timely notice to the regulator about the Incident.

2.12 Are organisations permitted to use any of the following measures to detect and deflect Incidents in their own networks in your jurisdiction?

Beacons (i.e. imperceptible, remotely hosted graphics inserted into content to trigger a contact with a remote server that will reveal the IP address of a computer that is viewing such content)
Use of beacons could arguably amount to unlawful intrusion into computer material but could be defensible under the affirmative defences of necessity or self-defence.

Honeypots (i.e. digital traps designed to trick cyber threat actors into taking action against a synthetic network, thereby allowing an organisation to detect and counteract attempts to attack its network without causing any damage to the organisation's real network or data)
Use of honeypots for detection purposes is likely permissible so long as it does not involve unlawful intrusion into the cyber threat actors' computers or invasion of their privacy (although these may in turn be defensible under the affirmative defences of necessity or self-defence). Use of honeypots for counter-attacks would amount to unlawful unlawful intrusion into the cyber threat actors' computers and other correlative offences.

Sinkholes (i.e. measures to re-direct malicious traffic away from an organisation's own IP addresses and servers, commonly used to prevent DDoS attacks)
Use of sinkholes for deflection purposes is likely permissible so long as it does not involve unlawful intrusion into the another person's computer, invasion of their privacy or interference with the ordinary functioning of their computer (although these may in turn be defensible under the affirmative defences of necessity or self-defence).

3 Specific Sectors

3.1 Does market practice with respect to information security (e.g. measures to prevent, detect, mitigate and respond to Incidents) vary across different business sectors in your jurisdiction? Please include details of any common deviations from the strict legal requirements under Applicable Laws.

Among those considered to be investing the most resources in cybersecurity are banks and credit card companies. This is likely due to them operating in a heavily regulated environment with a highly risk-averse regulator. At the other end of the spectrum are many small and medium businesses that often lack the resources for or awareness to, cybersecurity and compliance with the Israeli data security regulations.

3.2 Are there any specific legal requirements in relation to cybersecurity applicable to organisations in: (a) the financial services sector; and (b) the telecommunications sector?

Banks and credit card companies are subject to the cybersecurity requirements laid down by the Supervisor of Banks at the Israeli Central Bank. One of the operative requirements for banking corporations and credit card companies is to appoint a cyber-defence manager and define the board of directors' responsibilities in this realm. They are required to continuously examine the effectiveness of the various cyber-defence controls that they have established – using tools such as vulnerability reviews and controlled-intrusion tests.

Insurance companies and investment firms are subject to the cybersecurity requirements laid down by the Supervisor of Capital Markets, Insurance and Savings. They are required, for instance, to approve, at least once a year, a corporate policy on cybersecurity risk management. They must appoint a chief cybersecurity officer and conduct an annual assessment of the suitability of defensive measures to the organisation's overall cybersecurity risks.

The Regulation of Security in Public Bodies Law authorises the Israeli Security Agency and the National Cyber-defense Authority to issue binding directives to telecom organisations operating critical infrastructures on matters related to information security and cybersecurity. These directives are not published.

4 Corporate Governance

4.1 In what circumstances, if any, might a failure by a company (whether listed or private) to prevent, mitigate, manage or respond to an Incident amount to a breach of directors' duties in your jurisdiction?

There has yet to develop any Israeli case law on the issue of directors' liabilities relating to cybersecurity, but directors' negligence on cybersecurity governance could amount to a breach of the directors' duty of care. Additionally, cybersecurity guidelines issued by the Supervisor of Banks and the Supervisor of Capital Market, Insurance and Savings do specifically impose duties of oversight on the board of directors of these covered entities. Failure to so do may amount to the directors breaching their duty of care.

4.2 Are companies (whether listed or private) required under Applicable Laws to: (a) designate a CISO; (b) establish a written Incident response plan or policy; (c) conduct periodic cyber risk assessments, including for third party vendors; and (d) perform penetration tests or vulnerability assessments?

Under the Israeli Protection of Privacy Law, certain organisations are required to appoint an information security officer. These organisations include public agencies, service providers who process five or more databases of personal data by commission for other organisations and organisations that are engaged in banking, insurance and credit evaluation.

Organisations that are subject to the Israel data security regulations must establish and maintain procedures for Incident response.

Organisations that are subject to the intermediate or high security levels under the data security regulations are required to perform cyber risk assessments. Organisations that are subject to the high security level are also required to conduct assessments to identify cybersecurity risks.

Any organisation that is subject to the data security regulations is required to oversee and supervise its vendors' data security compliance on an annual basis.

Finally, organisations that are subject to the high level of security are required to perform penetration tests once every 18 months.

4.3 Are companies (whether listed or private) subject to any specific disclosure requirements in relation to cybersecurity risks or Incidents (e.g. to listing authorities, the market or otherwise in their annual reports)?

All publicly traded companies are required to include in their periodic reports details of all types of risks that the company is exposed to in light of their line of business, the environment in which they operate and the characteristics unique to their operations. The Israeli Securities Authority recently published a circular emphasising a public company's duties of disclosure both of general cybersecurity risks that a company faces as well as of specific Incidents having material adverse effects on the company. Research conducted two years ago found that nearly half of the top 125 companies trading on the Tel Aviv Stock Exchange did not report cybersecurity as a risk.

4.4 Are companies (whether public or listed) subject to any other specific requirements under Applicable Laws in relation to cybersecurity?

We are not aware of any other requirements.

5 Litigation

5.1 Please provide details of any civil actions that may be brought in relation to any Incident and the elements of that action that would need to be met.

The most prominent civil action that may be brought against a legal entity in relation to an Incident is class action lawsuit in accordance with the Israeli Class Action Law, 5766-2006.

In order for the court to certify a class action suit, the representative plaintiff must prove that: (1) the action raises substantive questions of fact or in law common to all members of the putative class that were affected by the Incident, and that it is reasonably possible that such questions will be resolved in the class's favour; (2) under the circumstances of the case, a class action is the efficient and fair method to dispose of the dispute; (3) there are reasonable grounds to assume that the interests of all members of the class will be appropriately represented and conducted; and (4) there are reasonable grounds to assume that the interest of all members of the group will be represented and conducted in good faith.

In addition, any person or legal entity that suffered damages related to an Incident may assert a personal civil action based on several applicable laws; for example – invasion of privacy in accordance with the Protection of Privacy Law or for negligence in accordance with the Israeli Torts Ordinance.

5.2 Please cite any specific examples of cases that have been brought in your jurisdiction in relation to Incidents.

The Incident involving the vehicle monitoring company described in the answer to question 2.11 above has led to at least two class action suits filed against the company, alleging that the company negligently failed to safeguard consumer information.

In September 2017, a similar class action lawsuit was filed against Leumi Card Ltd., an Israeli credit card issuer, following a severe Incident in 2014 where former company employees had stolen vast amounts of information on credit card holders and tried to extort millions of shekels from the company. The class action lawsuit alleges that the company negligently failed to safeguard consumer information.

In April 2011, the Herzliya Magistrate Court awarded ILS 400,000 to a plaintiff for damages he suffered after the defendants infected his personal computer with a Trojan in the wake of a family dispute.

5.3 Is there any potential liability in tort or equivalent legal theory in relation to an Incident?

A person or entity responsible for safeguarding data against an Incident may arguably be liable in tort for failing to take the security measures required under the Israeli data security regulations in negligence or the tort of breach of a legal duty.

6 Insurance

6.1 Are organisations permitted to take out insurance against Incidents in your jurisdiction?

Yes, organisations are permitted to take out insurance against Incidents, and it is in fact becoming more common.

6.2 Are there any regulatory limitations to insurance coverage against specific types of loss, such as business interruption, system failures, cyber extortion or digital asset restoration? If so, are there any legal limits placed on what the insurance policy can cover?

There are no noteworthy regulatory limits.

7 Employees

7.1 Are there any specific requirements under Applicable Law regarding: (a) the monitoring of employees for the purposes of preventing, detection, mitigating and responding to Incidents; and (b) the reporting of cyber risks, security flaws, Incidents or potential Incidents by employees to their employer?

Israeli legislation does not specifically address the issue of monitoring and accessing employees' communications and files. This legislative gap has been filled by case law, the most notable being a judgment delivered by the Israeli National Labor Court in 2011, known as the Isakov case. The judgment expounded Israeli privacy law as applied to employers monitoring and accessing employees' communications and files. The decision sets forth the boundaries of permissible access to employee's email communications. The ruling also sets forth a stringent set of pre-requisites and conditions for permissible access.

There are no specific requirements under Applicable Law regarding the reporting of cyber risks or Incidents by employees. Such requirements can be contractually stipulated in an employment agreement. Arguably, they can also be interpreted, in appropriate circumstances, to be part of an employee's general fiduciary obligations towards the employer or part of an employee's duty to act in good faith.

7.2 Are there any Applicable Laws (e.g. whistle-blowing laws) that may prohibit or limit the reporting of cyber risks, security flaws, Incidents or potential Incidents by an employee?

We are not aware of any such laws.

8 Investigatory and Police Powers

8.1 Please provide details of any investigatory powers of law enforcement or other authorities under Applicable Laws in your jurisdiction (e.g. antiterrorism laws) that may be relied upon to investigate an Incident.

The Israeli Police is empowered with general authority to investigate crimes and to seize documents, objects and computer materials that can potentially serve as evidence relating to the commission of a crime. Seizure of computers and computer material used by a business for investigation purposes requires a court order.

The Israeli privacy regulator has investigative powers relating to violations of the Israeli Protection of Privacy Law, including issues relating to the cybersecurity of databases containing personal data.

The Israeli Wiretap Law authorises investigative and security authorities to surreptitiously obtain the content of real time communications, for national security purposes or for the purpose of preventing and investigating serious crime. Wiretaps sought for preventing and investigating serious crime are subject to court approval, which in exceptional cases can be sought after the fact.

The Israeli Telecom Data Law provides police and various other investigative bodies with the authority to apply to the court of lowest instance in Israel to seek a comprehensive order to surreptitiously receive metadata (but not the content) of telecommunications, for the purpose of search and rescue, investigating or preventing crime, or seizing property. If metadata is required urgently and a court order cannot be obtained in time, such metadata may be obtained for a limited period of 24 hours, without a court order, subject to approval by a senior police officer.

Recently, a proposal for a Cyber Defense and National Cyber Directorate Bill was published. It proposes granting far-reaching and unprecedented powers to the National Cyber Directorate, such as compelling organisations to produce any information or document required to handle cyber-attacks and authority to issue instructions to organisations, including instructions to carry-out acts on the organisation's computerised material, for the purpose of handling cyber-attacks.

8.2 Are there any requirements under Applicable Laws for organisations to implement backdoors in their IT systems for law enforcement authorities or to provide law enforcement authorities with encryption keys?

Section 11 of the General Security Service Law, 5762-2002 (the statute governing the operation of the Israeli Security Agency, colloquially known as "Shabak" or "Shin Bet"), grants the Prime Minister sweeping powers to order that metadata and non-real time

telecommunications be retained by telecom providers and surreptitiously made available to the Shabak.

Section 13 of the Communications Law (Telecommunication and Broadcasts), 5742-1982, provides that the Prime Minister may order telecom service providers to render services to police, security agencies and intelligence agencies, and to have the providers install devices, take measures or adapt their facilities to assist the authorities.

Haim Ravia is a Senior Partner and Chair of the Internet, Cyber and Copyright Practice Group at Pearl Cohen Zedek Latzer Baratz. Haim deals extensively with data protection and privacy, cyber and internet law, IT contracts, copyright, electronic signatures, and open source software. Haim was a member of the Israeli public commission for the Protection of Privacy, and was part of a governmental team that re-examined the Israeli law pertaining to personal information databases. Haim received an acknowledgment award from the Israel Chamber of Information System Analysts for pioneering and innovation in the Israeli internet. Practising internet and cyber law for over 20 years, Haim has also written numerous columns on internet law for *Globes* (a major Israeli financial newspaper), the *Israel Bar Association Magazine* and other publications. Haim also operates Israel's first legal website (www.law.co.il) and publishes commentaries on *Lexology*.

Pearl Cohen Zedek Latzer Baratz
Azrieli Sarona Tower
121 Menachem Begin Rd.
Tel-Aviv, 6701203
Israel

Tel: +972 3 303 9058
Fax: +972 3 303 9001
Email: HRavia@PearlCohen.com
URL: www.pearlcohen.com
www.law.co.il

Dotan Hammer is a Partner and member of the Internet, Cyber and Copyright Group at Pearl Cohen Zedek Latzer Baratz. Dotan regularly advises on Israeli data protection and privacy laws. Having completed his academic degree in computer science at the age of 19, later working as a software developer and a technological project leader, Dotan also counsels clients on the privacy and data protections aspects of software and SaaS user agreements and licensing, as well as on other IT law matters such as digital (electronic) signatures, copyright issues and open source matters. Dotan regularly contributes to Israel's first legal website (www.law.co.il), *Lexology* and other online publications.

Pearl Cohen Zedek Latzer Baratz
Azrieli Sarona Tower
121 Menachem Begin Rd.
Tel-Aviv, 6701203
Israel

Tel: +972 3 303 9037
Fax: +972 3 303 9001
Email: DHammer@PearlCohen.com
URL: www.pearlcohen.com
www.law.co.il

ICLG.com

Current titles in the ICLG series

Alternative Investment Funds
Anti-Money Laundering
Aviation Law
Business Crime
Cartels & Leniency
Class and Group Actions
Competition Litigation
Construction & Engineering Law
Copyright
Corporate Governance
Corporate Immigration
Corporate Investigations
Corporate Recovery & Insolvency
Corporate Tax
Cybersecurity
Data Protection
Employment & Labour Law
Enforcement of Foreign Judgments
Environment & Climate Change Law
Family Law
Financial Services Disputes
Fintech
Foreign Direct Investments
Franchise
Gambling
Insurance & Reinsurance
International Arbitration
Investor-State Arbitration
Lending & Secured Finance
Litigation & Dispute Resolution
Merger Control
Mergers & Acquisitions
Mining Law
Oil & Gas Regulation
Outsourcing
Patents
Pharmaceutical Advertising
Private Client
Private Equity
Product Liability
Project Finance
Public Investment Funds
Public Procurement
Real Estate
Sanctions
Securitisation
Shipping Law
Telecoms, Media and Internet Laws
Trade Marks
Vertical Agreements and Dominant Firms

@ICLG_GLG

The International Comparative Legal Guides are published by global legal group