ICLG

The International Comparative Legal Guide to:

Cybersecurity 2019

2nd Edition

A practical cross-border insight into cybersecurity work

Published by Global Legal Group, with contributions from:

Advokatfirmaet Thommessen AS
Allen & Overy LLP
Angara Abello Concepcion Regala & Cruz Law Offices
Bagus Enrico & Partners
Boga & Associates
BTG Legal
Christopher & Lee Ong
Cliffe Dekker Hofmeyr Inc
Creel, García-Cuéllar, Aiza y Enríquez, S.C.
Eversheds Sutherland
Ferchiou & Associés
Gikera & Vadgama Advocates
Gouveia Pereira, Costa Freitas & Associados, S.P. R.L.
JIPYONG LLC
King & Wood Mallesons
Latham & Watkins LLP
Lee, Tsai & Partners Attorneys-at-Law
LT42 – The Legal Tech Company
Maples and Calder
Mori Hamada & Matsumoto
Niederer Kraft Frey Ltd.
Nyman Gibson Miralis
Pearl Cohen Zedek Latzer Baratz
R&T Asia (Thailand) Limited
Rajah & Tann Singapore LLP
Simmons & Simmons LLP
Siqueira Castro Advogados
Stehlin & Associes
Synch
Templars
USCOV | Attorneys at Law

glg
global legal group

glg
global legal group

Contributing Editors
Nigel Parker & Alexandra Rendell, Allen & Overy LLP

Sales Director
Florjan Osmani

Account Director
Oliver Smith

Sales Support Manager
Toni Hayward

Editor
Sam Friend

Senior Editors
Suzie Levy
Caroline Collingwood

Chief Operating Officer
Dror Levy

Group Consulting Editor
Alan Falach

Publisher
Rory Smith

Published by
Global Legal Group Ltd.
59 Tanner Street
London SE1 3PL, UK
Tel: +44 20 7367 0720
Fax: +44 20 7407 5255
Email: info@glgroup.co.uk
URL: www.glgroup.co.uk

GLG Cover Design
F&F Studio Design

GLG Cover Image Source
iStockphoto

Printed by
Ashford Colour Press Ltd.
October 2018

ISBN 978-1-912509-38-6
ISSN 2515-4206

Strategic Partners

General Chapters:

Country Question and Answer Chapters:

South Africa

Fatima Ameer-Mia

Cliffe Dekker Hofmeyr Inc

Christoff Pienaar

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:

At present, the current legal framework relating to cybercrime in South Africa is a hybrid of different pieces of legislation and the common law. Offences relating to cybercrime are primarily regulated under the Electronic Communications and Transactions Act 25 of 2002 ("**ECT Act**").

It has been recognised in South Africa that the current hybrid legal framework relating to cybercrimes and cybersecurity (in particular the common law, which develops on a case-by-case basis) has not kept up with the dynamic nature of technology and international standards. Accordingly, in September 2015, the first draft Cybercrimes and Cybersecurity Bill ("**Cybercrimes Bill**") was published in the South African parliament for comment. The most recent version of the Cybercrimes Bill [B6 of 2017] has recently been tabled in parliament but has not yet been promulgated into law.

The Cybercrimes Bill, once effective, will, *inter alia*, consolidate and codify numerous existing offences relating to cybercrime as well as create a variety of new offences which do not currently exist in South African law. The Cybercrimes Bill also deals with penalties for such cybercrime offences, provides for the powers of investigation, search, access and seizure in relation to prosecution of such offences, and regulates jurisdiction of the courts.

It is important to note that once the Cybercrimes Bill is in effect, it will repeal the relevant provisions in the ECT Act relating to cybercrime offences and cybersecurity.

We therefore set out the current legal framework below, as well as how this may differ under the pending legislation.

Hacking (i.e. unauthorised access)

Yes. Hacking is recognised as an offence under section 86(1) of the ECT Act, which states that it is an offence to intentionally access or intercept data without the appropriate authority of permission to do so. This also applies to unauthorised interference with data as contained in section 86(2) of the ECT Act. Under the ECT Act, the maximum penalty is a fine (unspecified) or imprisonment for a period not exceeding 12 months.

Under the Cybercrimes Bill, the offence of hacking is more broadly defined as it encompasses the unlawful and intentional access to data, a computer program, a computer data storage medium, or a computer system (section 2(1)). Under the Cybercrimes Bill, the maximum penalty is a fine (unspecified) or imprisonment for a period not exceeding five years (or both).

Denial-of-service attacks

Yes. Section 86(5) of the ECT Act states that any person who commits any of the acts described in sections 86(1)–86(4) with the intent to interfere with access to an information system so as to constitute a denial, including a partial denial, of service to legitimate users is guilty of an offence.

For the sake of completeness:

- section 86(1) – see discussion above in relation to hacking;
- section 86(2) – criminalises the unlawful intentional interference with data in a way which causes such data to be modified, destroyed or otherwise rendered ineffective;
- section 86(3) – makes it an offence to unlawfully produce, sell, offer to sell, procure for use, design, adapt for use, distribute or possess any device, including a computer program or a component, which is designed primarily to overcome security measures for the protection of data, or performs any of those acts with regard to a password, access code or any other similar kind of data with the intent to unlawfully utilise such item to contravene this section; and
- section 86(4) – makes it an offence to utilise any device or computer program mentioned in section 86(3) in order to unlawfully overcome security measures designed to protect such data from access thereto.

Under the ECT Act, the maximum penalty for contravening section 86(5) is a fine (unspecified) or imprisonment for a period not exceeding five years.

Phishing

Yes. Phishing is recognised as an offence under section 87(2) of the ECT Act, which provides that a person who commits any of the acts described in sections 86(1)–86(5) for the purpose of obtaining an unlawful advantage by causing fake data to be produced with an intent that it would be considered or acted upon as if it were authentic is guilty of offence. The maximum penalty under the ECT Act is a fine (unspecified) or imprisonment for a period not exceeding five years.

Phishing can also be prosecuted under the common law offences of theft and fraud. The maximum penalty imposed would depend on which court hears the case (which would depend on a variety of factors, the quantum of the claim being one). If the case is prosecuted in the Magistrate's Court, the court can impose a fine or imprisonment for a maximum period of 15 years in terms of its penal jurisdiction. If the case is heard in the High Court of South Africa, the court has wider discretion and may impose any fine or term of imprisonment which they deem appropriate in the circumstances.

Under the Cybercrimes Bill, there are separate offences for cyber fraud, cyber forgery and uttering and cyber extortion (sections 8, 9 and 10) which all attempt to deal with forms of phishing. A court which convicts a person of such an offence (where a penalty is not prescribed by any other law) can impose a sentence which the court deems appropriate and which is within that court's penal jurisdiction.

Infection of IT systems with malware (including ransomware, spyware, worms, trojans and viruses)

Yes. See the discussion above in respect of denial-of-service attacks. Section 87(1) relating to computer-related extortion, fraud and forgery of the ECT Act is also relevant as it states that it is an offence to perform or threaten to perform any of the acts described in section 86, for the purpose of obtaining any unlawful proprietary advantage by undertaking to cease or desist from such action, or by undertaking to restore any damage caused as a result of those actions.

Under the ECT Act, the maximum penalty imposed for contravention of section 86(4) or 87 is a fine (unspecified) or imprisonment for a period not exceeding five years.

Under the Cybercrimes Bill, there are separate offences for unlawful acts (in respect of software or hardware tools), as well as unlawful interference with data, a computer program, a computer data storage medium or a computer system (which is construed broadly enough to specifically include malware).

Under the Cybercrimes Bill, the maximum penalty for contravention of these sections is a fine (unspecified) or imprisonment for a period not exceeding 10 years (or both).

Possession or use of hardware, software or other tools used to commit cybercrime (e.g. hacking tools)

Yes. See the discussion above in respect of denial-of-service attacks. Section 86(3) of the ECT Act is relevant and the maximum penalty which can be imposed for contravention of section 86(3) is a fine or imprisonment for a period not exceeding 12 months.

Under the Cybercrimes Bill, it is an offence under section 4(1) to unlawfully and intentionally possess, manufacture, assemble, obtain, sell, purchase, make available or advertise any software or hardware tool for purposes of contravening certain other section of the Cybercrimes Bill. The maximum penalty for contravention of this section is a fine (unspecified) or imprisonment for a period not exceeding 10 years (or both).

Identity theft or identity fraud (e.g. in connection with access devices)

Yes. Section 87 of the ECT Act (which deals with computer-related extortion, fraud and forgery) is relevant and criminalises the actions of a person who performs or threatens to perform any of the acts in section 86 for the purpose of obtaining any unlawful proprietary advantage, or obtaining any unlawful advantage by causing fake data to be produced with the intent that it be considered or acted upon as if it were authentic. If the offender uses an access device to breach certain security measures and then uses the data unlawfully, then the offender will have contravened section 87 and 86 of the ECT Act. As stated above, the maximum penalty imposed for contravention of section 87 is a fine (unspecified) or imprisonment for a period not exceeding five years.

Identity theft or fraud can also be prosecuted under the common law offence of "theft" or "fraud". The sentencing jurisdiction would operate the same as discussed above in relation to "phishing".

Depending on the nature of the offence, it may also be possible to prosecute identity theft or fraud as an infringement of copyright under copyright laws.

Under the Cybercrimes Bill, there are separate offences for cyber fraud, cyber forgery and uttering and cyber extortion (sections 8, 9 and 10) which are broad enough to cover identity theft or fraud. A court which convicts a person of such an offence (where a penalty is not prescribed by any other law) can impose a sentence which the court deems appropriate and which is within that court's penal jurisdiction.

Electronic theft (e.g. breach of confidence by a current or former employee, or criminal copyright infringement)

Yes. Electronic theft may constitute an offence under section 86(1) of the ECT Act relating to unlawful access to data (see the discussion above in relation to hacking). It can also be prosecuted under the common law offence of theft.

Breach of confidence by a current/former employee would be actionable as a common law delict (tort), but not necessarily as a criminal offence.

With regards to criminal copyright infringement, the Copyright Act 98 of 1978 makes provision for criminal penalties, including a fine (a maximum of R5,000 per infringement) and/or imprisonment of up to three years for a first conviction. The maximum fine and/or imprisonment penalty for a second conviction is R10,000 and/or five years.

See also the discussion above in relation to hacking with regards to the Cybercrimes Bill and electronic theft.

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

The ECT Act also criminalises attempting to commit any of the offences in the ECT Act or aiding and abetting those offences (section 88). The same penalties would apply as if the offence was successfully perpetrated.

Under the Cybercrimes Bill there are numerous new offences relating to "malicious communications". For example, it will be an offence to disseminate a data message which advocates, promotes or incites hate, discrimination or violence against a person or group of persons. "Revenge porn" will also constitute an offence under the Cybercrimes Bill (where a naked image of a person is shared electronically without their consent). The infringement of copyright (through the use of peer-to-peer file sharing) is also an offence under the Cybercrimes Bill.

Failure by an organisation to implement cybersecurity measures

Under the current legislative framework, there is no law which imposes a duty to implement cybersecurity measures on an organisation.

However, the Protection of Personal Information Act 4 of 2013 ("**POPI Act**"), which was promulgated in 2013 but which has not yet commenced, does contain obligations for responsible parties (data controllers) to implement reasonable technical and organisational measures to safeguard personal information in their possession or control against unauthorised access, which will likely involve cybersecurity measures. The POPI Act further imposes administrative fines as well as punitive penalties for infringement of its provisions.

The Cybercrimes Bill imposes extensive cybersecurity obligations on electronic communications service providers, financial institutions, payment system institutions and any company, entity or person who is declared by the Minister of State Security to own or control a critical information structure. The Cybercrimes Bill establishes various cybersecurity structures such as the 24/7 point of contact, the Cybersecurity Hub and nodal points to promote the reporting, investigation and prosecution of Incidents of cybercrime.

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

Section 90 of the ECT Act lists the instances where South African courts will have extra-territorial jurisdiction in respect of cyber-related offences. This includes where the offence was committed in South Africa, where any preparatory act towards the offence was committed in South Africa, where the offence was committed by a citizen, resident or person carrying on business in South Africa or where the offence was committed on board any ship or aircraft registered in South Africa or on a voyage or flight to or from South Africa at the time the offence was committed.

Under the Cybercrimes Bill, the extraterritorial jurisdiction provisions are more extensive and even where an offence is committed outside of South Africa, a South African court will have jurisdiction if the person charged: is a citizen or ordinary resident of South Africa, was arrested in South Africa (or onboard a vessel registered in South Africa); or is a company or body of persons incorporated or registered in South Africa. An offence shall also be deemed to have been committed in South Africa under the Cybercrimes Bill if the act or commission affects or is intended to affect any person in South Africa or the perpetrator is found to be in South Africa; or if the perpetrator is not extradited by South Africa.

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?

There are no provisions in the ECT Act which deal with exceptions or mitigation of sentences. This would need to be considered by a court on a case-by-case basis.

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.

Certain terrorism offences may arise in relation to cybersecurity or an Incident. South Africa does have in place legislation criminalising acts of terrorism, but it is broad enough to cover a multitude of scenarios. The offence of treason is a common law offence and defined as "any conduct unlawfully committed by a person owing allegiance to a state with the intention of: (i) overthrowing the government of the Republic; (ii) coercing the government by violence into any action or inaction; (iii) violating, threatening or endangering the existence, independence or security of the Republic; and (iv) changing the constitutional structure of the Republic". The offence of treason may therefore also be construed broadly enough to include an Incident. We are not aware of any specific prosecutions in the cybersecurity context.

Under the Cybercrimes Bill, there is a new offence which relates to computer-related terrorist activity as the propagation of terrorist activities to recruit new members, disseminating information on how to make bombs or weapons, online co-ordination of terrorist attacks and any activity aimed at causing destruction, destabilisation or threatening national or international security.

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.

The legislative frameworks in South Africa that are relevant to cybersecurity are set out below:

- The right to privacy is enshrined in section 14 of the Constitution of South Africa, 1996 and states that "everyone has the right to privacy, which includes the right not to have their privacy of their communications infringed".
- In order to give effect to the right to privacy, the POPI Act was promulgated. The POPI Act is data protection legislation primarily modelled on the EU general data protection laws. Importantly, it establishes the Information Regulator and confers various powers, duties and functions including monitoring and enforcing compliance by public and private bodies and handling complaints in respect of contraventions of the POPI Act. It also establishes a comprehensive compliance framework and places cybersecurity obligations on responsible parties to secure the integrity and confidentiality of personal information in its possession or control by taking appropriate, reasonable technical and organisational measures to prevent unlawful access. The substantive provisions of the POPI Act are not yet in effect. The commencement date of the POPI Act is imminent.
- The ECT Act, as discussed in section 1 above, regulates electronic communications and transactions and is the primary legislation currently in force which criminalises cyber-related offences.
- The Cybercrimes Bill, as discussed in section 1 above, which is not yet in force, aims to consolidate and put in place a comprehensive cybersecurity framework and provides for the criminalisation of a broad range of cyber-related crimes.
- The Regulation of Interception of Communications and Provision of Communications-related Information Act 70 of 2002 ("**RICA**") regulates the interception and monitoring of direct and indirect communications. RICA contains exceptions relating to where interception and monitoring takes place with the consent of the parties involved or where it is carried out by law enforcement personnel.

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 is anticipated to exceed the requirements of the Directive.

There is no legislation in force which specifically relates to cybersecurity requirements applicable to critical infrastructure at present.

However, the Cybercrimes Bill (sections 58–60) will put in place measures to designate national critical information infrastructures and the mechanisms established to deal exclusively with the protection of such critical infrastructure. Information infrastructures will be declared as national critical information infrastructures if it appears that the information is of such a strategic nature that the interference, damage or loss thereof may prejudice state security, public health, the

rendering of essential services, economic stability or create a public emergency. There are procedures which the Minister of Security must follow before information infrastructures can be declared critical.

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.

Once the POPI Act comes into operation, the responsible party (similar to data controller) will be required to take appropriate reasonable technical and organisational measures to prevent unlawful access to personal information in its possession or control (section 19). This obligation will include taking measures to monitor, detect, prevent or mitigate Incidents. As the POPI Act is not yet in effect, the Information Regulator has not published any regulations or guidance on what measures are required to be taken.

The King IV Report on Corporate Governance for South Africa – 2016 ("**King IV**") is a set of voluntary principles in the area of corporate governance. Companies listed on the Johannesburg Stock Exchange are, however, required to comply with King IV by law. In particular, King IV has a specific focus on the oversight of information and technology management. The board of the company is specifically tasked to make sure it proactively monitors cyber Incidents and ensure that it has systems and processes in place from a cybersecurity perspective.

The Cybercrimes Bill also places obligations on electronic communication service providers (which includes financial institutions and any entity or person who is declared by the Minister of State Security to own or control a critical information structure) which become aware that its electronic communications network is being used to commit an offence to immediately report the matter in the prescribed manner to the South African Police Services and preserve all information/evidence that will be relevant to the investigation of the offence.

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.

Not at this stage, as the provisions of the POPI Act are not yet in force. The Cybercrimes Bill has also not been promulgated into law yet.

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 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 (e.g. malware signatures, network vulnerabilities and other technical characteristics identifying an Incident or cyber attack methodology); and (d) whether any defences or exemptions exist by which the organisation might prevent publication of that information.

Under current law, there is no duty to report Incidents to a regulatory or other authority.

Once the POPI Act comes into operation, section 22 provides that responsible parties must inform both the Information Regulator and the affected data subjects (unless the identity of such data subjects cannot be established) in writing as soon as reasonably possible that there is a breach or suspected breach – where there are reasonable grounds to believe that personal information of a data subject has been accessed or acquired by an unauthorised person. The notification must contain sufficient information to enable the data subject to take protective measures against potential consequences of the Incident. The Information Regulator may also direct the responsible party to publicise such Incident.

2.6 If not a requirement, are organisations permitted by Applicable Laws to voluntarily share information related to Incidents or potential Incidents 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?

There is no prohibition under current laws which would prevent organisations from voluntarily sharing information relating to Incidents with regulatory authorities in South Africa or outside of South Africa, provided such information is not subject to confidentiality restrictions, deemed classified or otherwise restricted.

The POPI Act is, however, not yet in operation, so the Information Regulator has not published any regulations or guidance notes on this issue.

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.

Yes, see the answer to question 2.5 above.

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?

At this stage, the reporting and notification obligation under the POPI Act will only apply to the extent that the Incident involves personal information. IP addresses and email addresses may constitute personal information. Once the POPI Act comes into operation, the Information Regulator may also publish regulations or exemptions on this issue.

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

Under the POPI Act, the Information Regulator (http://www.justice.gov.za/inforeg/) is responsible for enforcing the requirements.

Under the Cybercrimes Bill, the following authorities are relevant:

- the South African Police Services;
- the State Security Agency; and
- the National Prosecuting Authority.

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

The Information Regulator may impose administrative fines on responsible parties to a maximum of R10 million. Depending on the offence, the POPI Act also provides for fines and imprisonment not exceeding 10 years.

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

The POPI Act and Cybercrimes Bill are not yet in force and accordingly no enforcement action has been taken. Once the POPI Act comes into force, there will be a grace period of one year (which may be extended for up to three years) for responsible parties to comply with the provisions of the POPI Act.

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.

While there are no strict legal requirements under Applicable Laws which require different business sectors to address cybersecurity differently, certain sectors such as financial services (in particular banks and insurers who hold licences) tend to be more incentivised to avoid the cost and reputational impact of Incidents. As the POPI Act has been promulgated (but not yet effective) for a few years now, many organisations' cybersecurity practice is driven not just by "compliance" but also promoting good business practices. Once the POPI Act comes into force, the Information Regulator may publish industry-specific Codes of Conduct for different business sectors.

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?

No, not at present.

However, the Cybercrimes Bill will place obligations on electronic communication service providers (which includes financial institutions and any entity or person who is declared by the Minister of State Security to own or control a critical information structure) which become aware that its electronic communications network is being used to commit an offence to immediately report the matter in the prescribed manner to the South African Police Services and preserve all information/evidence that will be relevant to the investigation of the offence.

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?

See the discussion above under question 2.3 relating to King IV, which places obligations on the board of directors of the company to make sure it proactively monitors cyber Incidents and ensure that it has systems and processes in place from a cybersecurity perspective.

While the principles in King IV are voluntary (except for listed companies), failure by a company to prevent, mitigate, manage or respond to an Incident amount to a breach of directors' duties both under the common law and the Companies Act 71 of 2008 ("**Companies Act**").

Under the common law, a breach of fiduciary duties may apply, and the director can be held liable for any losses, damages or costs. Section 76 of the Companies Act sets out standards of directors conduct and that a director must always act in good faith, for a proper purpose, in the best interest of the company and with a degree of reasonable care, skill and diligence. Failure to prevent, mitigate, manage or respond to an Incident may amount to a breach of directors' duties under the Companies Act.

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?

No, there are no Applicable Laws which require companies to satisfy any of the specific requirements above. However, see the discussion above under question 2.3 relating to King IV, which places obligations on the board of directors of the company to make sure it proactively monitors cyber Incidents and ensures that it has systems and processes in place from a cybersecurity perspective.

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)?

There are no additional requirements other than what has been set out under questions 2.5 and 2.7 above.

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

No, there are no other specific 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.

There are a variety of civil actions which may be brought in relation to an Incident; the most relevant would probably be a claim for compensation (or damages) under a delictual action (*action lex aquila* – similar to tort). The claimant would need to claim against the organisation or individual which caused the Incident. In order to be entitled to compensation in damages, the claimant would need to prove: (i) a wrongful act or omission (i.e. the Incident); (ii) caused by negligence/fault/breach of duty of care; and (iii) actual monetary loss on the part of the claimant.

It is also conceivable that an Incident would, depending on the circumstances, give rise to a claim for breach of contract where the particular Incident constituted a breach of contract between the parties.

Section 99 of the POPI Act also provides for civil remedies in terms of which a data subject or the Information Regulator may institute a civil action for damages against a responsible party for breach of the provisions of the POPI Act (as referred to in section 73) whether or not there is intent or negligence on the part of the responsible party.

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

As far as we are aware, there have not been any specific cases in relation to Incidents brought in South Africa.

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

Yes; see the answer to question 5.1 above.

6 Insurance

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

Yes, although this is still relatively new in South Africa and the market has been slow to take up cyber-risk insurance cover (because South Africa has been slow in promulgating its data protection and cybersecurity legislation). Typically, this sort of insurance would cover business interruption, system failures, cyber extortion, etc.

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?

No, there are no regulatory limits on what the insurance policy can cover. The general rules of insurance would apply.

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?

No, there is no legislation which requires the monitoring of employees for the purposes of preventing, detecting, mitigating and responding to Incidents. Monitoring of employees' use of email and internet access, for example, will involve the processing of personal information and therefore the POPI Act (once effective) will apply.

RICA regulates the interception and monitoring of direct and indirect communications. RICA contains exceptions relating to where interception and monitoring takes place with the consent of the parties involved or where it is carried out by law enforcement personnel.

While there are no specific laws which place a duty on employees to report cyber risks, security flaws, Incidents or potential Incidents to their employers, once the POPI Act comes into effect it is likely that the employee (in the capacity of an operator) will have to notify the responsible party immediately if there are reasonable grounds to believe that the personal information of a data subject has been accessed by an unauthorised person.

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?

There are no Applicable Laws which may prevent or limit the reporting of Incidents by an employee. For whistle-blowers, the employee would need to satisfy the whistleblowing provisions in the Protected Disclosures Act 26 of 2000, one of which is that the subject matter of the disclosure falls into one or more categories. The categories include criminal offences and breach of a legal obligation, which may be appropriate for Incidents, although may not be wide enough to cover security flaws or mere risks.

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.

Currently, the South African Police Services has general law enforcement and investigatory powers to investigate an Incident. The Criminal Procedure Act 51 of 1977 sets out the procedure to be followed by the South African Police Services when investigating a criminal offence.

The POPI Act grants broad powers to the Information Regulator to, *inter alia*, commence an investigation at their own initiative, summon people to appear before it and give evidence, enter and search any premises, conduct interviews, carry out enquiries as the Information regulator sees fit and refer complaints to other bodies.

The Cybercrimes Bill establishes procedures which specifically cater for the investigation of cyber-related offences. The Cybercrimes Bill confers extensive powers to law enforcement authorities and other investigators in respect of access, search and seizure of articles involved in the commission of an offence. It also establishes a 24/7 point of contact and mutual legal assistance in the arena of cybercrimes (different law enforcement agencies working together to facilitate enforcement and compliance). The Cybercrimes Bill also authorises the President of South Africa to enter into agreements with foreign states for the provision of mutual assistance and co-operation relating to the investigation and prosecution of cyber-related offences.

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?

There are no such requirements under the Applicable Laws.

Fatima Ameer-Mia
Cliffe Dekker Hofmeyr Inc
11 Buitengracht Street
Cape Town, 8001
South Africa

Tel: +27 21 481 6374
Email: fatima.ameermia@cdhlegal.com
URL: www.cliffedekkerhofmeyr.com

Fatima Ameer-Mia is a senior associate in the Technology & Sourcing practice. Fatima specialises in commercial contracts, information technology, intellectual property and data protection law. She also has a special interest in the fields of e-commerce, information security and matters relating to cybercrime.

Fatima advises clients, both locally and internationally, in various sectors on their commercial and technology arrangements, including outsourcing, software licensing and development and systems integration.

She regularly advises on data protection and information security, including providing training, seminars, risk assessments and governance frameworks on cybersecurity and data protection laws.

Christoff Pienaar
Cliffe Dekker Hofmeyr Inc
11 Buitengracht Street
Cape Town, 8001
South Africa

Tel: +27 21 481 6350
Email: christoff.pienaar@cdhlegal.com
URL: www.cliffedekkerhofmeyr.com

Christoff Pienaar is Director and National Head of the Technology & Sourcing practice at Cliffe Dekker Hofmeyr Inc and is admitted to practise as an attorney of the High Court of South Africa and as a solicitor of the Senior Courts of England and Wales. He advises on commercial, information technology and intellectual property law. He specialises in information technology and commercial matters and has particular expertise in payment systems, technology outsourcing, business process outsourcing, data protection, information security, systems integration, hardware acquisitions and maintenance, IT consultancy services, managed services, disaster recovery services, software development and software licensing and support transactions. Christoff also advises on general commercial and intellectual property issues across a diverse range of industry sectors, especially financial services.

CDH
CLIFFE DEKKER HOFMEYR

Cliffe Dekker Hofmeyr Inc is one of the largest business law firms in South Africa, with more than 350 lawyers and a track record spanning over 164 years. The Technology & Sourcing practice of Cliffe Dekker Hofmeyr Inc is widely recognised as a market leader for its work with a large proportion of the top financial institutions in South Africa on their headline technology projects. The team is renowned across the technology and telecoms industries for its market-leading position in all of information technology, telecoms and privacy & data protection. The team handles domestic and global mandates and is involved in changes to key legislation affecting these sectors.

Other titles in the ICLG series include:

- Alternative Investment Funds
- Anti-Money Laundering
- Aviation Law
- Business Crime
- Cartels & Leniency
- Class & Group Actions
- Competition Litigation
- Construction & Engineering Law
- Copyright
- Corporate Governance
- Corporate Immigration
- Corporate Investigations
- Corporate Recovery & Insolvency
- Corporate Tax
- Data Protection
- Employment & Labour Law
- Enforcement of Foreign Judgments
- Environment & Climate Change Law
- Family Law
- Fintech
- 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
- Securitisation
- Shipping Law
- Telecoms, Media & Internet
- Trade Marks
- Vertical Agreements and Dominant Firms

glg global legal group

59 Tanner Street, London SE1 3PL, United Kingdom
Tel: +44 20 7367 0720 / Fax: +44 20 7407 5255
Email: info@glgroup.co.uk

www.iclg.com