International
Comparative
Legal Guides

Practical cross-border insights into cybersecurity

Cybersecurity 2023

Sixth Edition

Contributing Editor:
Edward R. McNicholas
Ropes & Gray LLP

ICLG.com

Expert Analysis Chapters

Q&A Chapters

Belgium


Roeland Lembrechts


Bart Van den Brande

Sirius Legal

1 Cybercrime

1.1 Would any of the following activities constitute a criminal or administrative 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)

Hacking, as an unauthorised access to an IT system, is criminalised under article 550*bis* of the Belgian Criminal Code (BCC).

The first distinction that must be made is between the basic crime (external and internal hacking) and the subsequent actions.

Article 550*bis* §1 relates to external hacking, while article 550*bis*, §2 relates to internal hacking. External hacking happens when a person not possessing any access rights knowingly intrudes in or maintains access to an IT system. The penalties are between six months and two years of imprisonment and/or a fine of between 208 EUR and 200,000 EUR. In cases where a fraudulent purpose is found, the maximum imprisonment is increased to three years.

Internal hacking happens when a person, who has access rights, exceeds those rights with a fraudulent purpose or with the purpose to cause damage. The penalties are between six months and three years of imprisonment and/or a fine of between 208 EUR and 200,000 EUR, e.g., employees abusing their access authority in the internal company network to use certain data for personal use can constitute internal hacking.

Subsequent actions are aggravating circumstances with increased penalties: imprisonment between one and five years; and/or a fine of between 208 EUR and 400,000 EUR. Subsequent actions can be stealing data, damaging an IT system or taking over an IT system to hack another system.

Instructing or commissioning a third party to commit hacking is punishable by between six months and five years of imprisonment and/or a fine of between 800 EUR and 1.6 million EUR.

Knowingly disseminating or using data obtained as a result of hacking is punishable with imprisonment between six months and three years and/or a fine of between 208 EUR and 800,000 EUR.

Denial-of-service attacks

Denial-of-service attacks are criminalised as computer sabotage, i.e., "knowingly and without authorisation, directly or indirectly introducing, altering or deleting data in an IT system, or changing by any other technological means the normal use of any data in an IT system" (article 550*ter*, §1 BCC).

The penalties are between six months and three years of imprisonment and/or a fine of between 208 EUR and 200,000 EUR. An attempt will be punished with the same penalties. If real damage is caused to the data in the computer system, the maximum imprisonment is increased to five years and the maximum fine to 600,000 EUR.

In cases with a fraudulent purpose or intention of causing harm, the penalty is increased to a maximum of five years' imprisonment. The same increase applies to attacks against critical infrastructures.

Causing a disruption of the correct working of an IT system is an aggravating circumstance: penalties are increased to between one and five years of imprisonment and/or a fine of between 208 EUR and 800,000 EUR.

Phishing

Phishing is, in most cases, punishable by article 504*quater* of the BCC, which sanctions computer-related fraud, i.e., "with fraudulent purpose, acquiring an unlawful economic advantage for himself or for another, by inputting, altering or deleting any data that is stored, processed or transmitted in a computer system, by means of an IT system or changing the normal use of data in an IT system by any other technological means".

The penalties are between six months and five years of imprisonment and/or a fine of between 208 EUR and 800,000 EUR. An attempt is punishable with six months to three years of imprisonment and/or a fine of between 208 EUR and 400,000 EUR.

Phishing may also be punishable under article 145, §3, 1° of the Electronic Communications Act of 13 June 2005 (ECA), prohibiting the fraudulent initiation of electronic communications, by means of an electronic communications network, with the intent to obtain an illegitimate economic advantage (for oneself or for another). This criminal offence is punishable with between one and four years of imprisonment and/or a fine of between 4,000 EUR and 400,000 EUR.

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

This is an act of computer sabotage (article 550*ter*, §1 BCC).

The same criminal penalties apply as those applicable to denial-of-service attacks.

Distribution, sale or offering for sale of hardware, software or other tools used to commit cybercrime

Article 550*bis*, §5 of the BCC provides a specific provision to penalise anyone who, illegitimately, imports, distributes, disseminates or otherwise makes available any tool, including computer data, primarily designed or modified to enable hacking.

The penalties are between six months and three years of imprisonment and/or a fine of between 208 EUR and 800,000 EUR.

Possession or use of hardware, software or other tools used to commit cybercrime

It is a criminal offence on its own to illegitimately possess, produce, sell, procure for use, import, distribute, disseminate or otherwise make available any instrument, including computer data, designed or adapted to enable hacking (article 550*bis*, §5 BCC) or computer sabotage (article 550*ter*, §4 BCC).

The penalties are between six months and three years of imprisonment and/or a fine of between 208 EUR and 800,000 EUR.

When this offence intercepts communication that is not publicly accessible, the penalties are between six months and two years of imprisonment and/or a fine of between 1,600 EUR and 80,000 EUR (article 314*bis*, §2*bis* BCC). If committed by a public officer, the penalties are between six months and three years of imprisonment and/or a fine of between 4,000 EUR and 160,000 EUR (article 259*bis*, §2*bis* BCC).

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

Identity theft is often a precursor to another criminal offence, e.g., theft, fraud, computer fraud, hacking or computer sabotage committed by using the stolen identity.

Identity fraud may directly be a criminal offence only if the fraud relates to the appropriation of the capacity of a civil servant or military functions, nobility titles, the title of attorney-at-law or the public use of a false family name (articles 227–231 BCC). Penalties are usually limited to fines (up to 8,000 EUR). In the case of publicly taking someone else's name, the penalties are between eight days and three months of imprisonment and/or a fine of between 200 EUR and 2,400 EUR (article 231 BCC). Identity fraud may also be punishable under article 210*bis* BCC, which punishes computer-related forgery. The penalties are between six months and five years of imprisonment and/or a fine of between 208 EUR and 800,000 EUR.

Additionally, identity theft or fraud can be qualified as an illegitimate process of personal data. Depending on the specific qualification, these offences are punished by the Belgian GDPR Act of 30 July 2018 with a fine of between 2,000 EUR and 120,000 EUR (article 222), 800 EUR to 160,000 EUR (article 227) or 4,000 EUR to 240,000 EUR (article 223).

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

There is no general qualification for electronic theft. Although there has been discussion, case law ruled that, e.g., theft of computer data can be punished under the general definition of theft (article 431 BCC).

As a subsequent action to theft, according to articles XI.304 and XV.105 of the Belgian Code of Economic Law, knowingly putting an unlawful copy of a computer program on the market or having it for commercial purposes, or putting on the market or having resources for commercial purposes that are exclusively intended for the unauthorised person to facilitate the removal or circumvention of technical provisions to protect a computer program, is punishable with imprisonment between one and five years.

Other intellectual properties are secured by articles XV.103–XV.106 of the Belgian Code of Economic Law with imprisonment between one and five years and/or a fine of between 4,000 EUR and 800,000 EUR in cases of infringement (piracy and counterfeit) with fraudulent and malicious purpose.

Overall, remedies for copyright infringements can be found under title 9 and 10 of book XI of the Belgian Code of Economic Law.

Unsolicited penetration testing (i.e. the exploitation of an IT system without the permission of its owner to determine its vulnerabilities and weak points)

Unsolicited penetration testing is punished in the same way as hacking. It is sufficient that the hacker knows that he is not entitled to enter the IT system. The fact that there would be no damage or malicious intent is in principle irrelevant for criminalisation. Even the hacking attempt will be punished with the same penalties as a completed hacking.

"The white hat hackers" and "penetration testers" must be careful. The very broad moral element in the use and possession of hacker tools (article 550*bis*, §5 BCC) constitutes a criminal offence, even when they are used with the permission of the owner of the hacked IT system. This means that for persons who, as a penetration tester, use programs that are mainly designed for hacking, there is a high chance of punishment under article 550*bis*, §5 BCC.

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

Article 210*bis* of the BCC punishes computer-related forgery, i.e., "by entering data that are stored, processed or transferred through an IT system, into an IT system, to change, to delete or to change the possible use of data in an IT system with any other technological means, which changes the legal scope of such data".

The penalties are between six months and five years of imprisonment and/or a fine of between 208 EUR and 800,000 EUR.

Anyone aware that the data obtained are inauthentic, but still uses such data, will be punished with the same sanctions as a perpetrator of forgery.

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

There is usually no extraterritorial application of Belgian laws.

Article 3 of the BCC provides that the criminal courts shall be competent for all crimes in Belgian territory. To localise a criminal offence, Belgium applies the ubiquity doctrine, which provides that a criminal offence is situated in all places where there is a constitutive element to the offence.

This theory is supplemented with the principle of indivisibility, which allows courts to take into consideration all elements that are indivisibly connected with a criminal offence located in Belgium and to declare themselves competent with regard to a co-perpetrator located in a foreign country.

In the context of war crimes and crimes against humanity, the Belgian criminal law provisions apply extraterritorially, e.g., in case of terrorism. The General Data Protection Regulation (GDPR) applies extraterritorially as per the criteria in article 3.2.

1.3 Are there any factors that might mitigate any penalty or otherwise constitute an exception to any of the above-mentioned offences (e.g. where the offence involves "ethical hacking", with no intent to cause damage or make a financial gain)?

A court may consider mitigating circumstances, such as the behaviour of the perpetrator, in determining the criminal sanctions or giving suspension/postponement of punishment. A pro-active notification or a declaration or plea of guilt may induce a court to impose lower penalties. An amicable settlement with the Public Prosecutor can also be possible.

Article 550*bis*, §1 BCC does not contain an exception that would allow ethical hacking. It is sufficient that the hacker

knows that he is not entitled to enter the IT system. The fact that there would be no damage or malicious intent is in principle irrelevant for criminalisation. Even the hacking attempt will be punished with the same penalties as a completed hacking.

2 Cybersecurity Laws

2.1 *Applicable Laws*: 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, data protection and e-privacy laws, intellectual property laws, confidentiality laws, information security laws, and import/export controls, among others.

Cybersecurity
- Act of 1 July 2011 on the security and protection of critical infrastructures (Critical Infrastructure Act).
- Directive (EU) 2016/1148 of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.
- COL 9/2017 on the investigation and prosecution policy regarding ransomware.
- Act of 7 April 2019 establishing a framework for the security of network and information systems of general interest for public security (Belgian NIS Act).
- Royal Decree of 12 July 2019, implementing the law of 7 April 2019, establishing a framework for the security of network and information systems of general interest for public security and the law of 1 July 2011 on the security and protection of critical infrastructures (NIS Royal Decree).
- Regulation (EU) 2019/881 of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity), information and communications technology, cybersecurity certification and repealing Regulation (EU) 526/2013 (Cybersecurity Act).
- Commission Implementing Regulation (EU) 2018/151 of 30 January 2018 laying down rules for the application of Directive (EU) 2016/1148 of the European Parliament and of the Council as regards further specification of the elements to be taken into account by digital service providers for managing the risks posed to the security of network and information systems, and of the parameters for determining whether an Incident has a substantial impact.
- Joint directive of the Ministers of Justice and of the Interior of 13 July 2021 on the measures necessary to include the management and security, traceability and integrity of the personal data and the information processed in the databases referred to in article 44/2 of the Police Service Act.
- Act of 20 July 2022 on Cybersecurity Certification of Information and Communication Technology and designating a National Cybersecurity Certification Authority.

Cybercrime
- BCC, as amended by the Act of 28 November 2000 on cybercrime, and the Act of 15 May 2006 on cybercrime.
- Belgian Code of Criminal Proceedings.
- ECA.
- Law of 21 December 2021 on transposing the Directive 2018/1972 of 11 December 2018 establishing the European Electronic Communications Code.

Data protection
- Article 22 of the Belgian Constitution.
- Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data, and the free movement of such data, and repealing Directive 95/46/EC (GDPR).
- Act of 3 December 2017 establishing the Data Protection Authority.
- Act of 30 July 2018 on the protection of natural persons with regard to the processing of personal data.
- Act of 5 September 2018 setting up the information security committee and amending various laws on the implementation of the General Data Protection Regulation and repealing Directive 95/46/EC.

Electronic communications, security of electronic communications and secrecy of electronic communications
- Article 22 of the Belgian Constitution.
- Directive 2002/58/EC of 12 July 2002 on privacy and electronic communications.
- ECA.
- Articles 259*bis* and 314*bis* of the BCC.
- Proposal for a Regulation concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC.
- Act of 20 July 2022 relating to the collection and retention of identification data and metadata in the sector of electronic communications and the provision of such data to the authorities.

Trust services and electronic signatures:
- Regulation (EU) 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market, and repealing Directive 1999/93/EC (eIDAS Regulation).
- Title 2 of Book XII of the Belgian Code of Economic Law.
- Act of 18 July 2017 on electronic identification.
- Act of 20 September 2018 on the harmonisation of the concepts of electronic signature and durable data carrier and the elimination of obstacles to the conclusion of contracts by electronic means.
- Royal Decree of 25 September 2018 on the harmonisation of the concepts of electronic signature and durable data carrier.

Intellectual property rights:
- Book XI of the Belgian Code of Economic Law.

Employee surveillance and BYOD:
- Article 22 of the Belgian Constitution.
- GDPR.
- ECA.
- Articles 259*bis* and 314*bis* of the BCC.
- Collective Bargaining Agreement No. 68 on employee camera surveillance.
- Collective Bargaining Agreement No. 81 on the protection of employees in relation to the surveillance of electronic online communication data.

Professional secrecy:
- Article 458 of the BCC.
- Act of 30 July 2018 on the protection of trade secrets.

Due diligence and due care:
- Articles 1382 and 1383 of the Belgian Civil Code.

2.2 *Critical or essential infrastructure and services*: Are there any cybersecurity requirements under Applicable Laws (in addition to those outlined above) applicable specifically to critical infrastructure, operators of essential services, or similar, in your jurisdiction?

Critical infrastructures are governed by the Critical Infrastructures Act (CIA). The personal scope of this Act is larger than that of Directive 2008/114/EC, which it implements in Belgian law. The CIA not only covers the energy and transportation sectors, but also the financial and electronic communications sectors.

There are no specific cybersecurity provisions in the CIA. It applies to all risks that may disrupt or destroy critical infrastructures, including cyber risks. Critical infrastructures must establish and execute a security plan, which may include cybersecurity measures.

The Belgian Cyber Security Act of 7 April 2019 (CSA) implements the NIS-Directive, applicable for operators of essential services and digital service providers, and designates the Centre for Cybersecurity Belgium (CCB) as the single point of contact for cybersecurity. This Act provides a wide range of powers and means for the implementation, monitoring and sanctioning of obligations under the NIS-Directive, e.g., security plans, annual internal audits, triennial external audits and administrative and criminal sanctions.

2.3 *Security measures*: Are organisations required under Applicable Laws to take measures to monitor, detect, prevent or mitigate Incidents? If so, please describe what measures are required to be taken.

Operators of essential services must take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems that they use in their operations, e.g., security plan, annual internal audit, triennial external audit, etc. (articles 20–23 CSA).

Digital service providers must identify and take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of their network and information systems. They shall take into account the following elements: (a) the security of systems and facilities; (b) Incident handling; (c) business continuity management; (d) monitoring, auditing and testing; and (e) compliance with international standards (articles 33–34 CSA).

Critical infrastructures must establish and implement a security plan (BPE) (article 13 CIA). This obligation implicitly includes Incident prevention and handling.

Providers of electronic communications services or electronic communications networks must implement adequate measures to manage the security risks in relation to their services or networks, including measures to mitigate the impact of security Incidents in relation to the end-users and other connected networks (article 107/2, §1 ECA).

Taking into account the state of the art, the controller and processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk (article 32 GDPR).

Qualified and non-qualified trust service providers shall take appropriate technical and organisational measures to manage the risks posed to the security of the trust services they provide (article 19 eIDAS Regulation).

The general principles of due diligence and due care will, in all likelihood, induce organisations to implement measures to prevent and handle Incidents in order to avoid or limit claims for damages. It does not, however, explicitly impose Incident prevention and handling.

2.4 *Reporting to authorities*: 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.

Operators of essential services immediately report all Incidents that have a significant impact on the availability, confidentiality, integrity or authenticity of the network and information systems on which the essential service or services it provides depend on. This notification is simultaneously made to the national CSIRT, the sectoral government, or its sectoral CSIRT, and the Directorate General Crisis Centre of the Ministry of Interior Affairs.

The notification is required even if the operator only has partial access to the relevant information to determine whether the Incident has a significant impact (articles 24–25 CSA).

Digital service providers have the same duty for the services offered by them in the European Union. The notification is made in accordance with the implementing Regulation 2018/151 of 30 January 2018 on a secured platform (articles 35–36 CSA) and should contain information to determine whether the potential cross-border impact of the Incident is significant.

The controller under the GDPR shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the Belgian Data Protection Authority, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

The notification must include the following information:

- the nature of the personal data breach;
- contact details of the data protection officer (DPO) or other contact point;
- the likely consequences of the personal data breach; and
- the measures taken or proposed to be taken.

Providers of electronic communications services/networks are subject to a binding personal data breach notification with the Belgian Data Protection Authority and, if impacted, the end-user, unless the provider has implemented mitigation measures (article 107/3, §3 ECA). They must also notify the Belgian Institute for Post and Telecommunications and the end-users about special security risks (article 107/3, §1 ECA). Security Incidents must also be notified to the Belgian Institute for Post and Telecommunications (article 107/3, §2 ECA).

Trust service providers must notify the Belgian Ministry of Economic Affairs or the Data Protection Authority about any breach of security or loss of integrity that has a significant impact on the trust service (article 19 eIDAS Regulation).

Critical infrastructures must notify any Incident that imperils the security of the critical infrastructure to the Communication and Information Centre (article 14, §1 CIA).

2.5 *Reporting to affected individuals or third parties*: 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.

Article 34 of the GDPR: When a personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate this breach to the data subject without undue delay. The information provided must, at least, include contact details of the DPO, likely consequences and measures taken or to be taken.

Article 107/3, §1 of the ECA: If there is a particular risk of network security breaches, the undertakings providing a publicly available electronic communications service shall inform subscribers and the Institute. If the risk requires measures other than those that can be taken by the undertakings providing the service, they shall indicate any means of combatting that risk, including an indication of the expected costs.

Article 19 of the eIDAS Regulation: When it is likely to adversely affect a natural or legal person to whom the trusted service has been provided, the trust service provider shall notify the natural or legal person of the breach of security or loss of integrity without undue delay.

The nature and scope of information is different for each notification duty.

2.6 *Responsible authority(ies)*: Please provide details of the regulator(s) or authority(ies) responsible for the above-mentioned requirements.

The following regulators are responsible for enforcement (excluding criminal actions):

- Data protection: the Belgian Data Protection Authority.
- Electronic communications: the Belgian Institute for Post and Telecommunications.
- Trust services: the Ministry of Economic Affairs.
- Critical infrastructures: the Ministry of Interior Affairs.
- Operators of essential services and digital service providers: CCB; the Ministry of Economic Affairs; and sectoral governments.

2.7 *Penalties*: What are the penalties for not complying with the above-mentioned requirements?

The following penalties apply:

- Data protection: criminal penalties (indirectly to subsequent failures under article 226 of the Belgian GDPR Act) and administrative penalties (article 83, §4 GDPR).
- Electronic communications: criminal penalties (articles 107/3 and 145 ECA).
- Critical infrastructures: criminal penalties (article 26 CIA).
- Operators of essential services and digital service providers: criminal and administrative penalties (articles 51 and 52 Belgian CSA).

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

The Belgian Data Protection Authority has enforcement powers. More specifically, it can impose administrative fines on companies as well as conduct investigations. Additionally, in some cases, it is possible to make a claim to the courts for compensation for damage. The focus is currently mainly on prevention and awareness, with various government initiatives to increase maturity around cybersecurity. The data protection authority took its first series of decisions in 2020, including one decision with regard to taking adequate technical and organisational measures (decision 22/2020 of 8 May 2020).

The authority ruled that there was no infringement as a Master IT Service Agreement had been concluded with the processor with the necessary provisions under GDPR, the necessary internal risk assessment methods had been taken, the effectiveness of the elaborated procedures had been evaluated by annual internal and external audits, and the company acted in a transparent manner when reporting to the authority.

3 Preventing Attacks

3.1 Are organisations permitted to use any of the following measures to protect their IT systems in your jurisdiction (including to detect and deflect Incidents on their IT systems)?

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)
This is not explicitly forbidden. It is only when the IP address is considered to be personal data under the GDPR that the processing must be compliant with the GDPR. An informed consent can be required in that case. Beacons, fingerprints and cookies also require informed consent under the ECA if they are not merely functional and/or collect personal data.

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)
This is not explicitly forbidden.

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)
This is not explicitly forbidden.

3.2 Are organisations permitted to monitor or intercept electronic communications on their networks (e.g. email and internet usage of employees) in order to prevent or mitigate the impact of cyber attacks?

Organisations have a limited ability to intercept electronic communications, but in practice this is virtually impossible without committing a criminal act. Article 314*bis* of the BCC prohibits the deliberate interception, access or recording of communications in which one does not participate and without the consent of all participants.

Article 124 of the ECA prohibits the deliberate knowledge of the existence of that communication, the identification of persons and the processing of the electronic communications that was obtained (deliberately or not) without the consent of all participants. Exceptions are provided for this last article, for example, Collective Bargaining Agreement No. 81, which provides for such an exception when necessary to prevent computers of the organisation from being hacked. However, the correct application is a subject of discussion in case law and legal doctrine.

3.3 Does your jurisdiction restrict the import or export of technology (e.g. encryption software and hardware) designed to prevent or mitigate the impact of cyber attacks?

No, there is no explicit prohibition, except for the use of hacker tools, which is punishable by article 550*bis*, §5 of the BCC.

4 Specific Sectors

4.1 Does market practice with respect to information security vary across different business sectors in your jurisdiction? Please include details of any common deviations from the strict legal requirements under Applicable Laws.

The market practice in relation to Incident handling varies greatly depending on the sector and nature of the activities.

Typically, the financial sector has implemented strict information security measures.

4.2 Excluding the requirements outlined at 2.2 in relation to the operation of essential services and critical infrastructure, are there any specific legal requirements in relation to cybersecurity applicable to organisations in specific sectors (e.g. financial services or telecommunications)?

The telecommunications sector is subject to specific obligations under the ECA (articles 107/2 and 107/3).

Although these are technically not legal requirements, the financial services sector is subject to specific cybersecurity obligations in the context of prudential supervision by the National Bank of Belgium.

In addition to this, the financial services sector and the telecommunications sector, together with the sectors of energy, transport, finance, healthcare, water and digital infrastructure, are governed by the CIA, which imposes security obligations.

5 Corporate Governance

5.1 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' or officers' duties in your jurisdiction?

A director and/or officer may be held liable for a breach of his duties as a director if he fails to act with due care and due diligence.

5.2 Are companies (whether listed or private) required under Applicable Laws to: (a) designate a CISO (or equivalent); (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?

(a) There is no specific obligation to designate a CISO as such. Under the GDPR, it can be required to designate a DPO (article 37 GDPR). Operators of essential services and digital service providers are obliged to designate a contact point for the security of network and information systems (articles 23 and 34 CSA). The same obligation applies to critical infrastructures (articles 12 and 13 CIA).

(b) A written response plan or policy is required under articles 20 and 21 (operators of essential services) and article 33, §1, b) (digital service providers) of the CSA. Article 13 of the CIA requires that the operator is responsible for organising exercises and for updating the security plan. It may be required under the GDPR, depending on the company's individual context. This is the case under article 35, §7, d) of the GDPR when a data protection impact assessment is needed and may also be required as a general but implicit security measure under article 32 of the GDPR.

(c) The CSA explicitly requires an annual internal audit and a triennial external audit for operators of essential services (article 38, §1 and 2). Article 13, §6 of the CIA: The operator is responsible for organising exercises and for updating the BPE, based on the lessons learned from the exercises or from any change to the risk analysis. It may be required under the GDPR, depending on the company's individual context.

(d) *Idem* as (c).

5.3 Are companies (whether listed or private) subject to any specific disclosure requirements (other than those mentioned in section 2) in relation to cybersecurity risks or Incidents (e.g. to listing authorities, the market or otherwise in their annual reports)?

There are no other specific disclosure requirements for companies in relation to cybersecurity risks or Incidents. If cybersecurity risks or Incidents have a major financial impact, there is a disclosure requirement in relation to the financial impact (e.g., in the annual report). If they have an impact on personal data, there is a disclosure obligation to the Data Protection Authority.

6 Litigation

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

In the case of negligence, any person suffering damage may file an action to obtain compensation. That person is required to adduce evidence of the existence of negligence (which may be adduced by evidencing a breach of Applicable Laws), the damages suffered and the causal link between the negligence and the damage.

If the Incident is the result of an unfair market practice or a breach of data protection law, cease-and-desist proceedings are possible.

6.2 Please cite any specific examples of published civil or other private actions that have been brought in your jurisdiction in relation to Incidents.

Actions with regard to Incidents are brought to the Belgian Data Protection Authority (BDPA). The DPA and the Belgian Centre for Cyber Security (BCCS) are the two central authorities responsible for cybersecurity in Belgium.

Recently, the BDPA fined a mobile phone provider in a case of "sim swapping", where someone received the phone number and SIM card of another customer. For three days, the third party was able to record the complainant's personal phone traffic and calls, as well as all the linked accounts, such as Paypal and WhatsApp.

In 2021, Vivalia, an intermunicipal healthcare group in Wallonia, also fell victim to a large-scale cyber attack that

paralysed several departments. Up to 400 gigabytes of patient and employee information and IT systems were held hostage for several months. The cybercriminals demanded a ransom in exchange for the data. Investigations were led by the federal police and the prosecutor.

6.3 Is there any potential liability in tort (or equivalent legal theory) in relation to failure to prevent an Incident (e.g. negligence)?

Yes, see question 6.1.

7 Insurance

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

Cyber insurance is permitted and even encouraged in Belgium.

The number of Incidents has even led to a greater general awareness and demand for insurance against Incidents.

7.2 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 generally no legal or regulatory limitations in relation to insurance coverage, except the possibility for insurance against criminal penalties. Administrative fines may, however, be covered by insurance.

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. anti-terrorism laws) that may be relied upon to investigate an Incident.

Law enforcement authorities have a variety of investigatory powers at their disposal, including:

- conducting (international) network searches;
- the right to copy, block or seize electronic data;
- intercepting, localising and accessing electronic communications;
- imposing technical cooperation from persons with knowledge about the relevant IT systems; and
- under very specific circumstances, hacking and computer sabotage, as well as decryption.

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?

Organisations are not required to implement backdoors. However, law enforcement authorities may require any person with the relevant knowledge to provide them with encryption keys.

Roeland Lembrechts is a Master of Criminology (2005) and Master of Law (2009). He started his career in 2009 at the Bar of Mechelen with a broad focus on criminal, civil and corporate law, and specialised in contractual and non-contractual liabilities.
In addition, Roeland was active as a board member of the department of contract law at the Bar of Antwerp (2018–2019) and is secretary of the professional journal *Today's Lawyer*, a magazine that focuses on the lawyer as an ethical and innovative entrepreneur with a focus on digitising the profession. Roeland has a special interest in contract and liability law within the digital single market. He has been a certified DPO since 2017.

Sirius Legal
Veemarkt 70
2800 Mechelen
Belgium

Tel: +32 15 490 221
Email: roeland@siriuslegal.be
URL: www.siriuslegal.be

Bart Van den Brande has been a member of the Dutch-speaking Brussels Bar Association since 2001. Bart has worked at several well-known Brussels law firms and has built extensive expertise in media and advertisement law, market practices and consumer protection, intellectual property, internet and e-commerce, privacy and data protection, IT, software development and gambling law.
Parallel to his law practice, Bart was a part-time teaching assistant at Vrije Universiteit Brussel between 2005 and 2013. He is the author of several articles, is an experienced speaker at seminars and for training courses and is regularly asked to comment on current legal events in the national media. Several court cases handled by Bart were later published.

Sirius Legal
Veemarkt 70
2800 Mechelen
Belgium

Tel: +32 15 490 221
Email: bart@siriuslegal.be
URL: www.siriuslegal.be

Sirius Legal is a Belgian boutique law firm specialising in internet law, advertisement law, media and entertainment law, IP/IT, consumer protection, gambling and cybersecurity. The Sirius Legal team is a small and young but experienced team of law professionals that try to offer tailor-made solutions to a wide range of clients, ranging from multinationals to individual players.

www.siriuslegal.be

SIRIUS.LEGAL
BUSINESS LAW FIRM

ICLG.com

Current titles in the ICLG series

Alternative Investment Funds
Anti-Money Laundering
Aviation Finance & Leasing
Aviation Law
Business Crime
Cartels & Leniency
Class & Group Actions
Competition Litigation
Construction & Engineering Law
Consumer Protection
Copyright
Corporate Governance
Corporate Immigration
Corporate Investigations
Corporate Tax
Cybersecurity
Data Protection
Derivatives
Designs
Digital Business
Digital Health
Drug & Medical Device Litigation
Employment & Labour Law
Enforcement of Foreign Judgments
Environment & Climate Change Law
Environmental, Social & Governance Law
Family Law
Fintech
Foreign Direct Investment Regimes
Franchise
Gambling
Insurance & Reinsurance
International Arbitration
Investor-State Arbitration
Lending & Secured Finance
Litigation & Dispute Resolution
Merger Control
Mergers & Acquisitions
Mining Law
Oil & Gas Regulation
Patents
Pharmaceutical Advertising
Private Client
Private Equity
Product Liability
Project Finance
Public Investment Funds
Public Procurement
Real Estate
Renewable Energy
Restructuring & Insolvency
Sanctions
Securitisation
Shipping Law
Technology Sourcing
Telecoms, Media & Internet
Trade Marks
Vertical Agreements and Dominant Firms

The International Comparative Legal Guides are published by: global legal group