Topic 9

Legal, Regulations, Compliance and Investigations

Dr Diarmuid Ó Briain

Version: 3.0

Ollscoil Teicneolaíochta an Oirdheiscirt
South East Technological University

Dr Diarmuid Ó Briain

Table of Contents

Illustration Index

Index of Tables

1 Objectives

By the end of this topic, you will be able to:

- Define computer crime and its different classifications.
- Categorise the legal and ethical implications of cybercrime, intellectual property infringement, liability, and negligence in the context of cybersecurity.
- Analyse the legal considerations during the different phases of incident response as an organisation responds to a cybersecurity incident.
- Evaluate the effectiveness of different cybersecurity compliance and ethics programmes.

2 Introduction

In today's increasingly digital world, computer crime is a growing threat to individuals, businesses, and governments alike. From malware and phishing attacks to data breaches and ransomware, cybercriminals are constantly developing new and sophisticated ways to exploit vulnerabilities and steal valuable information.

Understanding computer crime is essential for protecting yourself, your organisation and Critical National Infrastructure (CNI) from these threats. This topic will explore the different types of computer crime, their impact, and the initiatives that are being taken to prevent and investigate them. It will also discuss the international treaties on computer crime and their implications.

3 Computer Crime

Computer crime encompasses a broad range of potentially illegal activities. It is generally divided into one of two types of categories:

- Crimes that target computer networks or devices directly
  - Malware (malicious code)
  - Denial Of Service (DoS) attacks
  - Computer viruses
- Crimes facilitated by computer networks or devices, the primary target of which is independent of the computer network or device:
  - Cyber stalking
  - Fraud and identity theft
  - Phishing scams
  - Information warfare

A computer can be a source of evidence. Even though the computer is not directly used for criminal purposes, it is an excellent device for record keeping, particularly given the power to encrypt the data. If this evidence can be obtained and decrypted, it can be of great value to criminal investigators.

3.1 Classifications of Cyber Crimes

Cybercrimes in general can be classified into four categories:

- **Individual Cyber Crimes**
  - This type of cybercrime targets individuals. It includes phishing, spoofing, spam, cyberstalking, and more.
- **Organisation Cyber Crimes**
  - The main target here are organisations. Usually, this type of crime is carried out by teams of criminals including malware attacks and DoS attacks.
- **Property Cybercrimes**
  - Such cybrcrimes target property such as credit cards or even intellectual property rights.
- **Society Cybercrimes**
  - This is the most dangerous form of cybercrime as it includes cyber-terrorism.

3.2 Specific Cyber crimes

The following cyber crimes are most prevalent in Operational Technology (OT) environments:

- **Phishing and Scam**
  - OT environments are often targeted by phishing attacks, as employees in these environments may have access to sensitive data and systems. Phishing emails can be used to trick employees into revealing confidential information or clicking on malicious links that can infect their computers with malware.
- **Ransomware Attacks**
  - Ransomware attacks are also a major threat to OT environments. Ransomware can encrypt critical data and systems, making them unavailable to operators. This can disrupt operations and lead to significant financial losses.
- **Hacking/Misusing Computer Networks**
  - Hackers may target OT environments to gain unauthorised access to systems and data, or to disrupt operations. This can be done for a variety of reasons, including financial gain, espionage, or sabotage.
- **OT-Specific Attacks**
  - There are also a number of OT-specific cyber attacks that can target OT environments. These attacks may exploit vulnerabilities in OT devices or protocols to gain access to systems, disrupt operations, or cause physical damage.

In addition to the above, other cyber crimes that can be prevalent in OT environments include:

- **Social Engineering Attacks**
  - Social engineering attacks are attempts to trick employees into revealing confidential information or performing actions that compromise security. These attacks can be very effective, as they exploit human psychology.
- **Malware Attacks**
  - Malware is malicious software that can be used to infect computers and systems. Malware can be used to steal data, disrupt operations, or cause physical damage.
- **DOS Attacks**
  - DoS attacks are attempts to make computer systems or networks unavailable to their intended users. DoS attacks can be used to disrupt operations or extort money from victims.
- **Cyber terrorism**
  - There is a growing concern among law enforcement that Internet problems and server scans are part of an organised effort by cyber terrorists, foreign intelligence services, or other groups to map potential security holes in critical systems.

It is important to note that the cyber threat landscape is constantly evolving, and new threats are emerging all the time. Organisations with OT environments need to be aware of the latest threats and take steps to mitigate them. This includes implementing security measures such as firewalls, intrusion detection systems, and access control lists. Organisations should also train their employees on cyber security best practices.

3.3 Initiatives in the fight against Cybercrime

While in this subsection the focus is on European, UK, US and Indian initiatives it is important to recognoise that there are similar efforts across the world.

3.3.1 Convention on Cybercrime

Across the world there is a scramble to enact laws that deal with Cybercrime. The ***Council of Europe (CoE) ETS No. 185 Convention on Cybercrime*** [1] is the only binding international instrument on this issue. It serves as a guideline for any country developing comprehensive national legislation against Cybercrime and as a framework for international cooperation between State Parties to this treaty. On 1 March 2006 the Additional Protocol to the Convention on Cybercrime came into force. Those States that have ratified the additional protocol are required to criminalise the dissemination of racist and xenophobic material through computer systems, as well as of racist and xenophobic-motivated threats and insults. Forty-three nations have signed the treaty. The Convention entered into force in the US in 2007.

3.3.2 ePrivacy Directive

Directive 2002/58/EC Privacy and Electronic Communications [2], the ePrivacy Directive, is an European Union (EU) directive that regulates the processing of personal data and the protection of privacy in the electronic communications sector. The directive covers a wide range of topics, including:

- The confidentiality of communications
- The use of cookies and other tracking technologies
- Direct marketing
- Spam
- Data retention
- Security measures

The ePrivacy Directive is one of the most important pieces of legislation governing privacy in the digital age. It has been credited with helping to protect the privacy of European citizens and businesses.

The ePrivacy Directive has the following key provisions:

Confidentiality of communications: The ePrivacy Directive prohibits the interception, listening, tapping, storage, or any other type of surveillance or interception of communications and traffic data without the consent of the users.

Cookies and other tracking technologies: The ePrivacy Directive requires websites to obtain the consent of users before storing or accessing information on their devices. This includes cookies, web beacons, and other tracking technologies.

Direct marketing: The ePrivacy Directive prohibits the sending of unsolicited commercial emails and SMS messages without the prior consent of the recipient.

Spam: The ePrivacy Directive prohibits the sending of unsolicited commercial emails.

Data retention: The ePrivacy Directive limits the amount of time that electronic communication providers can retain traffic data.

Security measures: The ePrivacy Directive requires electronic communication providers to implement appropriate technical and organisational measures to protect the personal data of their users.

The ePrivacy Directive is currently being revised by the European Commission. The proposed revision is expected to update the directive to reflect the latest technological developments and to strengthen the privacy protections for European citizens.

3.3.3 General Data Protection Regulation

The ***Directive (EU) 2016/1148, General Data Protection Regulation (GDPR)*** [3] is a regulation in EU law on data protection and privacy for all individuals within the EU and the European Economic Area (EEA). It also addresses the transfer of personal data outside the EU and EEA areas. The GDPR aims primarily to give control back to citizens and residents over their personal data and to simplify the regulatory environment for international business by unifying the regulation within the EU. The regulation has been in effect since May 25, 2018.

GDPR regulates the processing of personal data by both public and private organisations in the EU, including the transfer of personal data outside the EU. It gives individuals more control over their personal data and requires organisations to be more transparent about how they collect and use personal data. The GDPR also introduces a number of new requirements for organisations, including:

- Obtaining consent from individuals before collecting or processing their personal data
- Providing individuals with access to their personal data and the right to have their personal data erased
- Reporting data breaches to supervisory authorities within 72 hours
- Appointing a data protection officer if the organisation processes large amounts of personal data or sensitive personal data

GDPR is a complex piece of legislation, but it is important for all organisations that collect or process personal data to understand and comply with its requirements.

The key benefits of GDPR are:

- More control for individuals over their personal data: The GDPR gives individuals more control over their personal data, including the right to access, rectify, erase, and restrict the processing of their personal data.
- Greater transparency from organisations: The GDPR requires organisations to be more transparent about how they collect and use personal data.
- A more harmonised regulatory environment for businesses: The GDPR replaces the data protection directive of 1995, creating a more harmonised regulatory environment for businesses operating in the EU.

The GDPR is a significant step forward in the protection of personal data in the EU. It is important for all organisations that collect or process personal data to understand and comply with its requirements.

3.3.4 EU Cybersecurity Act

Regulation (EU) 2019/881, EU Cybersecurity Act [4] is seen as a means to unify the EU's cybersecurity into a single framework, with EU Agency for Cybersecurity (ENISA) as its main core It came into force on 28 June 2019 and has been implemented by all EU Member States. The Cybersecurity Act has two main functions:

- To strengthen the mandate of the ENISA.
- To establish a framework for the cybersecurity certification of Information and Communications Technology (ICT) products, services, and processes.

ENISA is responsible for supporting EU Member States in improving their cybersecurity capabilities. The Cybersecurity Act gives ENISA a number of new powers, including the power to:

- Provide advice and assistance to Member States on cybersecurity matters.
- Carry out risk assessments and threat analyses.
- Develop and promote cybersecurity best practices.
- Coordinate incident response activities.

The Cybersecurity Act also establishes a framework for the cybersecurity certification of ICT products, services, and processes. This framework is designed to help organisations to identify and choose secure ICT products, services, and processes. It also aims to promote innovation in the cybersecurity sector. Here are some of the key benefits of the EU Cybersecurity Act:

- It helps to improve the coordination and cooperation between EU Member States on cybersecurity issues.
- It provides a framework for the cybersecurity certification of ICT products, services, and processes, which can help organisations to choose and implement secure solutions.
- It strengthens the mandate of ENISA, which plays a vital role in supporting EU Member States in improving their cybersecurity capabilities.

3.3.5 EU Cyber Resilience Act

The ***EU 2022/0272(COD), EU Cyber Resilience Act (CRA)*** [5] sets out cybersecurity requirements for a range of hardware and software products placed on the EU market, including smart speakers, games, operating systems, etc. The Act aims to improve the cybersecurity of products with digital elements. The CRA applies to a wide range of products, including hardware, software, and ancillary services.

It imposes a number of requirements on manufacturers, importers, and distributors of these products, including:

- They must implement appropriate cybersecurity measures throughout the product's life cycle, from design and development to production, support, and maintenance.
- They must provide users with information about the cybersecurity risks associated with their products and how to mitigate them.
- They must report serious cybersecurity incidents to the competent authorities.

The CRA also establishes a number of other measures to improve the cybersecurity of products with digital elements, such as:

- A cybersecurity certification scheme for high-risk products.
- A common vulnerability disclosure framework.
- A coordinated response to cybersecurity incidents.

The CRA is expected to have a significant impact on the cybersecurity of products with digital elements in the EU. It is expected to help to reduce the number of cybersecurity incidents and to make it easier for users to choose and use secure products. Here are some of the key benefits of the EU Cyber Resilience Act:

- It helps to improve the overall cybersecurity of products with digital elements in the EU.
- It makes it easier for users to choose and use secure products.
- It reduces the number of cybersecurity incidents.
- It promotes innovation in the cybersecurity sector.
- It helps to strengthen the EU's cybersecurity resilience.

3.3.6 Digital Operational Resilience Act

Financial institutions present a particular cybersecurity risk and through ***Regulation (EU) 2022/2554, EU Digital Operational Resilience Act (DORA)*** [6] aims to strengthen the resilience of the EU financial sector to digital operational disruptions and threats. It came into force on 17 January 2023 and will apply to all financial entities in the EU from 17 January 2025. DORA sets out a number of requirements for financial entities, including:

- They must identify and assess their digital operational risks.
- They must implement appropriate measures to manage their digital operational risks, including measures to prevent, detect, respond to, and recover from digital operational incidents.
- They must test their digital operational resilience regularly.
- They must report digital operational incidents to their competent authorities.

DORA also establishes a number of other measures to improve the digital operational resilience of the EU financial sector, such as:

- A common cybersecurity incident reporting framework
- A coordinated response to digital operational incidents
- A cybersecurity awareness and training programme for financial entities

DORA is a significant step forward in the EU's efforts to improve the digital operational resilience of the financial sector. It is expected to help financial entities to better protect themselves from digital operational threats and to reduce the impact of digital operational incidents. Here are some of the key benefits of the EU Digital Operational Resilience Act:

- It helps to improve the overall digital operational resilience of the EU financial sector.
- It makes it easier for financial entities to manage their digital operational risks.
- It reduces the number of digital operational incidents.
- It promotes innovation in the cybersecurity sector.
- It helps to strengthen the EU's financial stability.

3.4 Initiatives in other countries

3.4.1 UK

Computer crimes are an offence in the UK under the ***Computer Misuse Act (CMA) 1990*** [7]. Offences can also arise under the ***Data Protection Act (DPA) 2018*** [8]. Here, the offence also involves the intent to secure unauthorised access to personal data, or under the ***Investigatory Powers Act (IPA) 2016*** [9], if the offence includes intentionally diverting communications without a legal authority to do so. In addition, the ***Fraud Act 2006*** [10], explicitly refers to phishing as an example of fraud by false representation. The ***Privacy and Electronic Communications (PECR) Regulations 2003*** [11] sit alongside the DPA 2018 providing specific privacy rights in relation to electronic communications.

The UK National Cyber Security Centre (NCSC) is a part of the UK's Government Communications Headquarters (GCHQ) intelligence agency and is responsible for protecting the UK from cyber threats. UK NCSC provides a range of services to the UK government, businesses, and individuals, including cyber threat intelligence and advice, incident response support as well as cyber security training and education.

3.4.2 USA

In the USA computer crimes are dealt with under federal legislation. The ***Computer Fraud and Abuse Act (CFAA), 1986*** [12] prohibits unauthorised access to computers and networks, as well as data theft and damage. To deal with theft of trade secrets for foreign powers the ***Economic Espionage Act (EEA), 1996*** [13] is employed. The ***Identity Theft and Assumption Deterrence Act (ITADA), 1998*** [14] prohibits the unauthorised use of personal information, such as Social Security numbers and credit card numbers. To ensure that financial institutions implement cybersecurity measures to protect customer data, the US government enacted the ***Gramm-Leach-Bliley Act (GLBA), 1999*** [15] and they require healthcare providers to implement cybersecurity measures to protect patient data via the ***Health Insurance Portability and Accountability Act (HIPAA), 1996*** [16].

In addition to federal law, most states in the USA also have their own computer crime laws. The US government takes computer crimes very seriously and has a number of agencies dedicated to investigating and prosecuting these crimes, including the Federal Bureau of Investigation (FBI), the Secret Service, and the Department of Justice.

The US Government Cybersecurity and Infrastructure Security Agency (CISA) is responsible for coordinating the government's response to cybersecurity incidents, providing guidance and assistance to critical infrastructure sectors, and developing and implementing cybersecurity policies and standards. CISA plays a vital role in coordinating the government's response to cybersecurity incidents, providing guidance and assistance to critical infrastructure sectors, and developing and implementing cybersecurity policies and standards.

3.4.3 India

In a similar way the Indian government has enacted a number of cybersecurity laws to protect the country from cyberattacks and other threats to its critical infrastructure and citizens. The most important Indian cybersecurity law is the ***Information Technology Act, 2000*** [17]. The IT Act is a comprehensive law that covers a wide range of cybersecurity issues, including unauthorised access to computers and networks, data theft and damage, and cybercrime.

Other important Indian cybersecurity laws include the ***Indian Penal Code, 1860 (IPC)*** [18] contains several provisions that can be used to prosecute cybercrimes, such as cheating, forgery, and defamation. The ***Information Technology (Amendment) Act, 2008*** [19] added new provisions to the IT Act, such as the requirement for certain businesses to appoint a Chief Information Security Officer (CISO). Additionally, the ***Information Technology Rules, 2011*** [20] prescribe specific cybersecurity measures that certain businesses and organisations must implement. Like the EU NIS, the ***Indian National Cyber Security Policy, 2013*** [21] provides a framework for protecting India's CNI from cyberattacks and the ***National Cyber Security Strategy, 2020*** [22] outlines India's vision for a safe and secure cyberspace.

These laws are enforced by a variety of government agencies, including the Indian Computer Emergency Response Team (CERT-In), the Ministry of Electronics and Information Technology (MeitY), and the Central Bureau of Investigation (CBI).

Table 1: The law fighting Cybercrime

Group	Document	Year	Body	Specific Purpose
Data Protection	General Data Protection Regulation (GDPR)	2016	EU	To strengthen the protection of personal data in the EU and to give individuals more control over their personal data.
	Data Protection Act (DPA) 2018	2018	UK	To protect the privacy of individuals and the confidentiality of their personal data.
	Identity Theft and Assumption Deterrence Act (ITADA), 1998	1998	US	To criminalise the unauthorised use of personal information, such as Social Security numbers and credit card numbers.
	Information Technology (Amendment) Act, 2008	2008	India	To amend the Information Technology Act, 2000, to add new provisions related to cybersecurity, such as the requirement for certain businesses to appoint a Chief Information Security Officer (CISO).
	Information Technology Rules, 2011	2011	India	To prescribe specific cybersecurity measures that certain businesses and organisations must implement.

Group	Document	Year	Body	Specific Purpose
Espionage	Economic Espionage Act (EEA), 1996	1996	US	To criminalise the theft of trade secrets with the intent to benefit a foreign power.

Group	Document	Year	Body	Specific Purpose
Financial	EU Digital Operational Resilience Act (DORA)	2022	EU	To establish a harmonised framework for digital operational resilience across the financial sector of the EU.
	Gramm-Leach-Bliley Act (GLBA), 1999	1999	US	To require financial institutions to implement cybersecurity measures to protect customer data.
Health	Health Insurance Portability and Accountability Act (HIPAA), 1996	1996	US	To require healthcare providers to implement cybersecurity measures to protect patient data.
General	Convention on Cybercrime	2001		Guideline for any country developing comprehensive national legislation against Cybercrime.
	Directive (EU) 2002/58/EC e Privacy	2002	EU	Regulates the processing of personal data and electronic communications.
	Privacy and Electronic Communications (PECR) Regulations 2003	2003	UK	To protect the privacy of individuals and the confidentiality of their electronic communications.
	Computer Fraud and Abuse Act (CFAA), 1986	1986	US	To criminalise unauthorised access to computer systems and data, unauthorised modification of data, and DOS attacks.
	Indian Penal Code, 1860 (IPC)	1860	India	To criminalise a wide range of offenses, including many that are relevant to cybersecurity, such as cheating, forgery, and defamation.

4 Intellectual Property

Is a term referring to a number of distinct types of legal monopolies over creations of the mind, both artistic and commercial, and the corresponding fields of law. Under intellectual property law, owners are granted certain exclusive rights to a variety of intangible assets, such as musical, literary, and artistic works; discoveries and inventions; and words, phrases, symbols, and designs. Common types of intellectual property include copyrights, trademarks, patents, industrial design rights and trade secrets in some jurisdictions.

4.1 Patent

This term refers to a right granted to anyone by the state (Government patent office) who invents or discovers any new and useful process, machine, article of manufacture, or composition of matter, or any new and useful improvement thereof.

A patent provides the right to exclude others from making, using, selling, offering for sale, or importing the patented invention for the term of the patent, which is usually 20 years from the filing date subject to the payment of maintenance fees.

Patents are the strongest form of IP and is a legally enforceable right to prevent others from using the invention for the period of the patent.

4.2 Trademark

A trademark is a distinctive sign or indicator used by an individual, business organisation, or other legal entity to identify that the products or services to consumers with which the trademark appears originate from a unique source, and to distinguish its products or services from those of other entities.

A trademark is designated by the following symbols:

- ™ Unregistered trade mark
- SM Unregistered service mark
- ® Registered trademark

The owner of a registered trademark may commence legal proceedings for trademark infringement to prevent unauthorised use of that trademark. However, registration is not required. The owner of a common law trademark may also file suit, but an unregistered mark may be protectable only within the geographical area within which it has been used or in geographical areas into which it may be reasonably expected to expand.

A service mark differs from a trademark in that the mark is used on the advertising of the service rather than on the packaging or delivery of the service, since there is generally no "*package*" to place the mark on, which is the practice for trademarks.

4.3 Copyright

Copyright is a form of intellectual property that gives the author of an original work exclusive right for a certain time period in relation to that work, including its publication, distribution and adaptation, after which time the work is said to enter the public domain. Copyright applies to any expressible form of an idea or information that is substantive and discrete and fixed in a medium.

Copyright protection extends to the following works:

- original literary, dramatic, musical or artistic works
- sound recordings and films
- broadcasts and TV programmes
- the typographical arrangement of published editions
- computer programmes
- original databases.

Copyright takes effect as soon as the work is put on paper, film, or other fixed medium such as CD-ROM, DVD, Internet, etc. No protection is provided for ideas while the ideas are in a person's mind. Copyright law protects the form of expression of ideas, not the ideas themselves.

Copyright is a weaker IP right than a patent but its duration is much longer. It typically applies for 50 – 70 years depending on the form of work.

4.3.1 Copyleft

Copyleft is a play on the word copyright to describe the practice of using copyright law to remove restrictions on distributing copies and modified versions of a work for others and requiring that the same freedoms be preserved in modified versions.

Copyleft is a form of licensing and can be used to modify copyrights for works such as computer software, documents, music and art. In general, copyleft licensing scheme, give every person who receives a copy of a work permission to reproduce, adapt or distribute the work as long as any resulting copies or adaptations are also bound by the same copyleft licensing scheme.

Common practice for using copyleft is to codify the copying terms for a work with a license. Any such license typically gives each person possessing a copy of the work the same freedoms as the author, including (from the Free Software Definition):

- the freedom to use the work
- the freedom to study the work
- the freedom to copy and share the work with others
- the freedom to modify the work, and the freedom to distribute modified and therefore derivative works

The GNU General Public License, originally written by Richard Stallman, was the first copyleft license to see extensive use, and continues to dominate the licensing of copylefted software.

4.4 Trade Secret

A trade secret is information that:

- Is not generally known to the public
- Confers some sort of economic benefit on its holder
- Is the subject of reasonable efforts to maintain its secret?

A company can protect its confidential information through non-competitive and Non-Disclosure Agreements (NDA) with its employees. The law of protection of confidential information effectively allows a perpetual monopoly in secret information. It does not expire as would a patent. The lack of formal protection, however, means that a third party is not prevented from independently duplicating and using the secret information once it is discovered.

4.5 International trade

International trade is exchange of capital, goods, and services across international borders or territories. It refers to exports of goods and services by a firm to a foreign-based buyer or importer.

International trade is in principle not different from domestic trade as the motivation and the behaviour of parties involved in a trade does not change fundamentally depending on whether trade is across a border or not. The main difference is that international trade is typically more costly than domestic trade. The reason is that a border typically imposes additional costs such as tariffs, time costs due to border delays and costs associated with country differences such as language, the legal system or a different culture.

The regulation of international trade is done through the World Trade Organisation (WTO) at the global level, and through several other regional arrangements such as the EU between member states, MERcado COmún del SUR (Spanish) Southern Common Market (MERCOSUR) in South America and the North American Free Trade Agreement (NAFTA) between the US, Canada and Mexico.

4.5.1 Encryption Export Control

Encryption export controls became a matter of public concern with the introduction of the PC. Phil Zimmermann's PGP cryptosystem and its distribution on the Internet in 1991 was the first major *'individual level'* challenge to controls on export of cryptography. The growth of electronic commerce in the 1990s created additional pressure for reduced restrictions. Shortly afterward, Netscape's SSL technology was widely adopted as a method for protecting credit card transactions using public key cryptography.

SSL-encrypted messages used the RC4 cipher, and used 128-bit keys. US government export regulations would not permit crypto systems using 128-bit keys to be exported.

The longest key size allowed for export without individual license proceedings was 40 bits, so Netscape developed two versions of its web browser. The "*US edition*" had the full 128-bit strength. The "*International Edition*" had its effective key length reduced to 40 bits by revealing 88 bits of the key in the SSL protocol. Acquiring the US domestic version turned out to be sufficient hassle that most computer users, even in the US, ended up with the '*International*' version, whose weak 40-bit encryption could be broken in a matter of days using a single personal computer.

Legal challenges by civil libertarians and privacy advocates, the widespread availability of encryption software outside the US, and the perception by many companies that adverse publicity about weak encryption was limiting their sales and the growth of e-commerce, led to a series of relaxations in US export controls, culminating in 1996 in President Bill Clinton signing the Executive order 13026 transferring the commercial encryption from the Munition List to the Commerce Control List. Furthermore, the order stated that, the software shall not be considered or treated as "*technology*" in the sense of Export Administration Regulations. This order permitted the US Department of Commerce to implement rules that greatly simplified the export of commercial and open source software containing cryptography.

4.5.2 Current status

4.6 Wassenaar Arrangement

The ***Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies*** [23] is a Multilateral Export Control Regime (MECR) with 42 participating countries.

It is the successor to the Cold war-era Coordinating Committee for Multilateral Export Controls (COCOM), and it was established on May 12, 1996, in the Dutch town of Wassenaar, near The Hague. The Wassenaar Arrangement is considerably less strict than COCOM, focusing primarily on the transparency of national export control regimes and not granting veto power to individual members over organisational decisions. A Secretariat for administrating the agreement is located in Vienna, Austria.

The Wassenaar Arrangement maintains a list of controlled items, which are goods, software, and technology that can be used for both civilian and military purposes. Participating states are required to implement export controls on these items in accordance with the Wassenaar Arrangement's guidelines.

The Wassenaar Arrangement is an important tool for preventing the proliferation of weapons of mass destruction and other sensitive technologies. It also helps to protect the security of participating states and their citizens.

The Wassenaar Arrangement is not legally binding, but participating states are committed to implementing its guidelines in good faith. The Wassenaar Arrangement also has a strong enforcement mechanism, which includes regular reviews of participating countries' export control systems and the possibility of sanctions for non-compliance.

4.6.1.1 The EU

European Council Regulation (EC) 428/2009 [24], of 5 May 2009, sets up an EU wide regime for the control of exports, transfer, brokering and transit of dual-use items (recast) is a regulation of the EU that establishes a common framework for the control of dual-use items. Dual-use items are goods, software and technology that can be used for both civilian and military purposes.

Regulation (EU) 2018/1922 of 10 October 2018 [25] amends Regulation (EC) 428/2009 to update the list of dual-use items that are subject to control, and it also makes some changes to the criteria that must be met in order to obtain an authorisation to export, transfer, broker or transit dual-use items.

4.6.1.2 The UK

After Brexit the UK replaced Regulation (EU) 2018/1922 with the ***Export Control Order 2020 (ECO 2020)*** [26]. The ECO 2020 implements the UK's obligations under various international export control regimes, including the Wassenaar Arrangement, the Nuclear Suppliers Group, and the Missile Technology Control Regime.

The ECO 2020 controls the export, transfer, and brokering of controlled items, which are goods, software, and technology that can be used for both civilian and military purposes. The ECO 2020 also controls certain items that are specifically designed or modified for military purposes.

The ECO 2020 contains a list of controlled items, which is similar to the list of controlled items in Regulation (EU) 2018/1922. However, there are some differences between the two lists. For example, the ECO 2020 list includes certain items that are not included in the EU list, such as certain types of encryption software.

4.6.1.3 The US

In the US, as of 2009, non-military cryptography exports are controlled by the Department of Commerce's Bureau of Industry and Security through the **Export Administration Regulations (EAR)** [11]. Some restrictions exist, even for mass market products, particularly with regard to export to "rogue states" and terrorist organisations. Militarised encryption equipment, TEMPEST-approved electronics, custom cryptographic software, and even cryptographic consulting services still require an export licence.

4.6.1.4 India

India has a number of different laws and regulations that govern the export of dual-use items. These include: the ***Foreign Trade (Development & Regulation) Act, 1992 [27]*** and the ***Export Control Guidelines, 2019*** as well as the Directorate General of Foreign Trade (Export Control) Notifications.

The Foreign Trade (Development & Regulation) Act gives the government the power to regulate the export of dual-use items through the Export Control Guidelines, 2019. These guidelines provide a list of dual-use items that are subject to export control. The guidelines also set out the criteria that must be met in order to obtain a licence to export dual-use items.

4.6.2 Export Control Summary

Table 2 outlines various regulations and acts from different countries concerning the control of dual-use goods.

Table 2: Export Control Summary

Document	Year	Body	Specific Purpose
European Council Regulation (EC) 428/2009: Dual-use export controls	2009	EU	To strengthen the protection of personal data in the EU and to give individuals more control over their personal data.
Regulation (EU) 2018/1922: The control of exports, transfer, brokering and transit of dual-use items	2018	EU	Update of the list of dual-use items that are subject to control, and it also makes some changes to the criteria that must be met in order to obtain an authorisation to export, transfer, broker or transit dual-use items.
Export Control Order 2020	2020	UK	Implements the UK's obligations under various international export control regimes, including the Wassenaar Arrangement, the Nuclear Suppliers Group, and the Missile Technology Control Regime.
Export Administration Regulations (EAR)	2009	US	Non-military cryptography export controls.
Foreign Trade (Development & Regulation) Act, 1992	1992	India	Regulate the export of dual-use items.

5 Liability and Negligence

Legal liability is the legal bound obligation to pay debts. A person is said to be legally liable when they are financially and legally responsible for something. Legal liability concerns both civil law and criminal law. Payment of damages usually resolved the liability. In commercial law, limited liability is a form of business ownership in which business owners are legally responsible for no more than the amount that they have contributed to a venture. If for example, a business goes bankrupt an owner with limited liability will not lose unrelated assets such as a personal residence (assuming they do not give personal guarantees). This is the standard model for larger businesses, in which a shareholder will only lose the amount invested (in the form of stock value decreasing).

Manufacturer's liability is a legal concept in most countries that reflects the fact that producers have a responsibility not to sell a defective product.

Negligence is a type of delectation or civil wrong. It can be considered the gap or difference between Actions where due diligence is expected and due care as defined in a policy. Or the gap between the policy and best practice or regulation.

Negligence is not the same as carelessness, because someone might be exercising as much care as they are capable of, yet still fall below the level of competence expected of them.

Through civil litigation, if an injured person proves that another person acted negligently to cause his injury, he can recover damages to compensate for his harm.

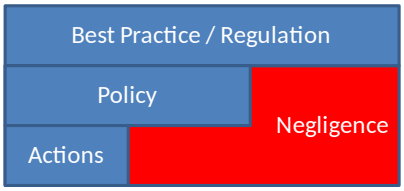

Figure 1: Negligence

6 Privacy

Privacy is the ability of an individual or group to seclude themselves or information about themselves and thereby reveal themselves selectively.

6.1 Data privacy

This refers to the evolving relationship between technology and the legal right to, or public expectation of privacy in the collection and sharing of data about one's self. Privacy concerns exist wherever uniquely identifiable data relating to a person or persons are collected and stored, in digital form or otherwise. In some cases these concerns refer to how data is collected, stored, and associated. In other cases the issue is who is given access to information. Other issues include whether an individual has any ownership rights to data about them, and/or the right to view, verify, and challenge that information. Various types of personal information often come under privacy concerns:

- Financial privacy
- Internet privacy
- Medical privacy
- Sexual privacy
- Political privacy

6.1.1 Examples of Privacy Laws

6.1.1.1 The EU

The ***EU Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data*** [28] was the initial EU directive which regulates the processing of personal data within the Union member states. It was replaced by ***Regulation (EU) 2016/679 General Data Protection Regulation (GDPR)*** [29] as a new EU law on data protection and privacy in the Union (EU) and the European Economic Area (EEA). It also addresses the transfer of personal data outside the EU and EEA areas. The GDPR aims primarily to give control back to citizens and residents over their personal data and to simplify the regulatory environment for international business by unifying the regulation within the EU. The regulation came into effect in May 25, 2018.

GDPR regulates the processing of personal data by both public and private organisations, including the transfer of personal data outside the EU. It gives individuals more control over their personal data and requires organisations to be more transparent about how they collect and use personal data.

6.1.1.2 The UK

The UK equivalent of the GDPR is the ***UK Data Protection Act 2018 (UK GDPR)*** [8]. It is the UK's implementation of the EU GDPR, which is a regulation in EU law on data protection and privacy. The UK GDPR came into force on 28 June 2018, the same day that the UK left the EU.

The UK GDPR is almost identical to the EU GDPR, but it makes some minor changes to reflect UK law. For example, the UK GDPR includes a definition of "special category data" that is slightly broader than the definition in the EU GDPR.

Like the EU GDPR, the UK GDPR applies to all organisations that process personal data of individuals in the UK, regardless of whether the organisation is based in the UK or not. It also applies to organisations that offer goods or services to individuals in the UK, or that monitor the behaviour of individuals in the UK.

6.1.1.3

6.1.1.4 The US

Due to the different legal tradition in the US, compared to the EU, which places a greater emphasis on individual liberty and less emphasis on government regulation means that the US is less inclinded to adopt comprehensive data protection laws. There is no single federal data protection law similar to GDPR; however, there are a number of federal and state laws that regulate the collection, use, and disclosure of personal data. Examples include the ***California Consumer Privacy Act (CCPA), 2018*** [30] and the ***Virginia Consumer Data Protection Act (VCDPA), 2023*** [31]. These laws give consumers the right to know what personal data is collected about them, to request access to that data, to have it deleted, and to opt out of the sale of their personal data. Similar laws exist in other US states such as Colorado, Connecticut and Utah; however, each of these laws vary in scope and complexity, but they all give consumers some rights over their personal data.

Apart from the state laws there are a number of federal laws that protect specific types of personal data, such as the **Health Insurance Portability and Accountability Act (HIPAA), 1996** [16] protects health data, the ***Gramm-Leach-Bliley Act (GLBA), 1999*** [15] protects financial data, the ***Fair Credit Reporting Act (FCRA) 1970*** [32] protects credit data, while the ***Children's Online Privacy Protection Act (COPPA), 1998*** [33] protects the personal data of children under the age of 13.

Since GDPR came into force there is growing support for a federal data protection law in the US. In 2022, the American Data Privacy and Protection Act (ADPPA), 2022 [34] passed through a committee of the US Congress with bipartisan support; however, it was never brought to a vote in the House of Representatives. The aim of ADPPA is to create a single federal data protection law for the US.

6.1.1.5 India

The ***Indian Digital Personal Data Protection Act (DPDP), 2023*** [35] is a comprehensive data protection law that was passed by the Indian Parliament in August 2023. It is similar to the EU GDPR in many ways. It gives individuals rights over their personal data and also requires organisations that process personal data to take steps to protect it and to ensure that it is processed in a fair and lawful way.

There are also some key differences between the DPDP Act and the GDPR. For example, the DPDP Act does not have a requirement for organisations to obtain explicit consent from individuals before processing their personal data. Additionally, the DPDP Act exempts certain types of organisations from its provisions, such as government agencies and small businesses.

The DPDP Act is enforced by the Data Protection Authority (DPA), which is a new independent body that has been set up under the Act. The DPA has the power to investigate complaints about breaches of the DPDP Act and to take action against organisations that are found to be in breach.

6.1.2 Privacy Summary

Table 3 provides a comparison of various data protection regulations and acts from different countries and regions.

Table 3: Privacy Summary

Document	Year	Body	Specific Purpose
Regulation (EU) 2016/679 General Data Protection Regulation (GDPR)	2016	EU	Addresses the transfer of personal data outside the EU and EEA areas.
UK Data Protection Act 2018 (UK GDPR)	2018	UK	Implements EU GDPR regulations in the UK.
Health Insurance Portability and Accountability Act (HIPAA)	1996	US	Protects health data.
Gramm-Leach-Bliley Act (GLBA)	1999	US	Protects financial data.
Fair Credit Reporting Act (FCRA)	1970	US	Protects credit data.
Children's Online Privacy Protection Act (COPPA)	1998	US	Protects the personal data of children under the age of 13.
Digital Personal Data Protection Act (DPDP), 2023	2023	India	Comprehensive data protection law that is similar to the EU GDPR.

6.2 Privacy at work

Today companies are under increasing pressure to monitor employees electronically, and workers should assume they are being watched. A large percentage of companies are now conducting some form of *active monitoring* of their employees, particularly E-mail monitoring.

Employees generally have a right to privacy based on a '*reasonable expectation of privacy'* but a written policy notifying employees of monitoring lifts somewhat the expectation of privacy."

This means that if an employee is led to expect something is private, such as e-mail communications, then that privacy cannot be violated. But, if the company informs its employees that, for example, e-mail sent over the company's network is monitored, then the employee can no longer claim an expectation of privacy.

The key for successfully managing the balancing act between privacy and security is for firms to make clear to their employees that their privacy at work is limited.

It's not really about Big Brother watching either, e-mail is quite often used as a tool of harassment and employers have a duty to be sure harassment isn't being propagated. For the company to exercise its responsibility it needs to monitor or at least record the e-mail traffic.

7 Incident Management

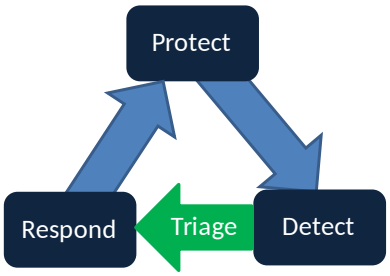

Figure 2: Incident Management

This is about proactively preparing for and reacting to an incident. Proactive preparation involves the preparation of policies to deal with possible events and the implementation of a continuous cycle of auditing and improvement of these policies.

Reaction is the measures carried out on the detection of an incident. How the incident was detected, what triage classification and prioritisation was carried out and how the response was conducted.

Good source of information are the:

- NIST SP 800-61 Computer Security Incident Handling Guide [36]
- Software Engineering Institute (SEI)
  - Handbook for Computer Security Incident Response Teams (CSIRT) [37]

7.1 Collection of Digital Evidence

Evidence is subject to strict rules regarding its admissibility in courts. To be presented, recorded in the court record and considered in the verdict, evidence must be:

- **Relevant**
  - It must pertain to the actual case.
- **Material**
  - It must prove or disprove facts that impact the question before the court.
- **Competent**
  - It must be proven to actually be what it purports to be.

With digital evidence, "*do no harm*". Do not start open the log files, do not shut down the system, etc. Do as little as possible beyond disconnecting the system from the network and protecting it until it can be handed over to Gardaí or police or other appropriate law enforcement.

- Do not turn off the system as data in volatile, Random Access Memory (RAM) will be lost.
- Disconnect the system from the network as this prevents a hacker from covering their tracks by deleting evidence like log files.
- Do not use the system for any reason, such as running programs as data in memory may be unwittingly overwritten.
- Do not open files to examine them as the time records for access and modification will be overwritten.
- Document everything done to the system subsequent to the incident.

7.1.1 Preserving digital evidence

The best way to preserve digital evidence in its original state is to copy it from one machine to another via a private network connection. The source computers memory should be transferred to the target computer first. The contents of the source computer's hard disk should be copied to the target computer as a bit level image not file by file to create an exact copy of the source disk data including empty space (which may include deleted residual data). A number of specialist software programs exist for this purpose.

A forensic duplicate consists of every bit of the raw bitstream stored in an identical format (e.g. using an identical disk).

On the other hand, a qualified forensic duplicate is a copy where every bit of information is still stored, but perhaps in a different form, such as an ISO image.

Both are submissable as evidence, but the '*best evidence*' should be used, e.g. the original disk.

7.2 Evidence Chain of Custody

Chain of Custody is the chronological documentation, showing the seizure, custody, control, transfer, analysis, and disposition of evidence, physical or electronic.

Who – What – When – Where – How

7.3 Process of Investigation

Identify:

1. Suspects
2. Systems
3. Witnesses
4. Investigative team
5. Search warrants

For filesystems, analyse the ownership and the modification records. What were the Means, Opportunity and Motives (MOM) of personnel can assist in narrowing down suspects to a crime.

Are there any Modus Operandi (MO), methods, choice of software or applications that may point to a particular set of habits, traits, or practices that can be used to identify a suspect.

7.4 Interviewing Suspects

Once a suspect has been identified and s/he is in a position to be interviewed, it is imperative that this conversation is planned beforehand. Will interview or interrogation techniques be applied? The basic difference between interview and interrogation is that an interview is conducted in a cordial atmosphere where a suspect or witness is more comfortable physically and psychologically. When a person is questioned in an uncomfortable atmosphere under psychological pressure, it is then an interrogation.

7.5 Hearsay

Hearsay evidence is generally inadmissible in court. This means that a witness cannot testify about what someone else said outside of court, unless the statement falls into one of the exceptions to the hearsay rule. If a witness starts to give hearsay evidence, they can be interrupted and asked to stop by the judge or by one of the lawyers in the case.

There are exceptions to the hearsay rule however, such as:

- **Admissions and confessions**: If the accused makes a statement that admits or confesses to a crime, this statement is admissible in court, even though it is hearsay. This is because it is assumed that someone would not make a statement against their own interests unless it was true.
- **Dying declarations**: If someone is dying and they make a statement about the circumstances of their death, this statement is admissible in court, even though it is hearsay. This is because it is assumed that someone who is about to die is more likely to tell the truth.
- **Business records**: Business records, such as invoices and receipts, are generally admissible in court, even though they are hearsay. This is because business records are usually created and kept in a reliable manner.
- **Public records**: Public records, such as birth certificates and death certificates, are generally admissible in court, even though they are hearsay. This is because public records are created by government officials and are considered to be reliable.

Exceptions to the hearsay rule are complex and there are a number of factors that a judge will consider when deciding whether to admit hearsay evidence in court.

The Law Reform Commission of Ireland has recommended that the hearsay rule be reformed and have proposed that the rule should be abolished. Instead the commission propose that judges should have a discretion to exclude hearsay evidence in certain circumstances. However, the hearsay rule has not yet been reformed in Ireland.

The courts in both the UK and India for example have a discretion to admit hearsay evidence even if it does not fall into one of the established exceptions. This discretion is exercised sparingly and only in cases where the court is satisfied that it is in the interests of justice to admit the evidence.

In the US the exceptions already mentioned include further exceptions such as statements made in furtherance of a conspiracy, statements made by witnesses prior to trial, and statements made by experts.

Additionally, the courts in the US have a discretion to admit hearsay evidence even if it does not fall into one of the established exceptions. This discretion is exercised sparingly and only in cases where the court is satisfied that it is in the interests of justice to admit the evidence.

8 Compliance and ethics

8.1 Regulatory Compliance

Historically in all countries there have been periods of business and government excesses and subsequent legal, public and political reaction. All countries have imposed regulation of compliance to prevent and punish companies who participate in corporate malpractice.

8.1.1 The EU

Directive (EU) 2006/43/EC, the Audit Directive [38]. The Audit Directive sets out minimum standards for the statutory audit of Public-Interest Entities (PIE) in the EU. The directive requires PIEs to have their annual financial statements audited by an independent auditor and to publish a corporate governance statement.

In addition to the EU Audit Directive, there are a number of other EU laws and regulations that are relevant to corporate governance and anti-corruption. For example, the ***Regulation (EU) 596/2014, the Market Abuse Regulation*** [39] prohibits insider trading and market manipulation and the ***Regulation (EU) 2016/679 General Data Protection Regulation (GDPR)*** [29] sets out rules for the processing of personal data.

Companies operating in the EU should be aware of all of the relevant EU laws and regulations, and should take steps to ensure that they are in compliance.

8.1.2 The UK

The ***UK Bribery Act 2010*** [40], is a law that makes it illegal to bribe anyone, anywhere in the world. It is one of the toughest anti-bribery laws in the world and applies to all UK companies and individuals, regardless of where they are located or operating. The Bribery Act creates four offences:

- Bribery of another person
- Bribery of a foreign public official
- Failure of a commercial organisation to prevent bribery
- Bribery of a foreign public official to obtain or retain business or an advantage in the conduct of business.

The Act also introduces strict liability for commercial organisations whose employees or other associated persons engage in bribery, even if the organisation itself did not know about or benefit from the bribery. This means that commercial organisations must have adequate procedures in place to prevent bribery.

The Bribery Act has been successful in reducing bribery in the UK. Since it came into force, the Serious Fraud Office (SFO) has prosecuted over 200 individuals and companies for bribery offences.

8.1.3 The US

The ***US Foreign Corrupt Practices Act (FCPA)*** [41] is an anti-bribery provision makes it unlawful for a US citizen, and certain foreign issuers of securities, to make a corrupt payment to a foreign official for the purpose of obtaining or retaining business for or with, or directing business to, any person. The law also requires publicly traded companies to maintain records that accurately and fairly represent the company's transactions. It also requires these companies to have an adequate systems of internal accounting controls.

The ***US Sarbanes–Oxley Act (SOX)*** [42] is the US Public Company Accounting Reform and Investor Protection Act. It was enacted as a reaction to a number of major corporate and accounting scandals such as at Enron and a number of other US companies which cost investors billions of dollars when the share prices of affected companies collapsed, shook public confidence in the nation's securities markets.

The legislation sets standards for all US public company boards, management and public accounting firms. It does not apply to privately held companies. The act contains 11 titles, or sections, ranging from additional corporate board responsibilities to criminal penalties, and requires the Securities and Exchange Commission (SEC) to implement rulings on requirements to comply with the new law.

Additionally, the ***US Gramm-Leach-Bliley Act (GLBA)*** [15] is the US Financial Services Modernisation Act to allow commercial banks, investment banks, securities firms and insurance companies to consolidate. One area of the act is the protection of the privacy of consumer information held by these organisations.

8.1.4 India

There are a number of Indian laws and regulations that are relevant to corporate governance and anti-corruption. The ***Prevention of Corruption Act, 1988 (POCA)*** [43] criminalises bribery and other forms of corruption while the ***Companies Act, 2013 (CA) [44]*** sets out standards for corporate governance and financial reporting.

8.2 Basel II and III

Basel II [45] is a series of recommendations on banking laws and regulations are issued by the Basel Committee on Banking Supervision. This international committee encourages contacts and cooperation among its members and other banking supervisory authorities. Basel II creates an international standard that banking regulators can use when creating regulations about how much capital banks need to put aside to guard against the types of financial and operational risks banks face. Generally speaking, these rules mean that the greater risk to which the bank is exposed, the greater the amount of capital the bank needs to hold to safeguard its solvency and overall economic stability.

Basel III [46] augmenting and superseding parts of the Basel II standards, it was developed in response to the deficiencies in financial regulation revealed by the financial crisis of 2007–08. It is intended to strengthen bank capital requirements by increasing minimum capital requirements, holdings of high quality liquid assets, and decreasing bank leverage.

8.2.1 Regulatory Compliance Summary

Table 4 provides an overview of various regulations and acts related to corporate governance, financial crime, and data protection from different jurisdictions.

Table 4: Regulatory Compliance

Document	Year	Body	Specific Purpose
Directive (EU) 2006/43/EC, the Audit Directive	2006	EU	Sets out minimum standards for the statutory audit of Public-Interest Entities (PIE) in the EU.
Regulation (EU) 596/2014, the Market Abuse Regulation	2014	EU	Prohibits insider trading and market manipulation.
Regulation (EU) 2016/679 General Data Protection Regulation (GDPR)	2016	EU	Sets out rules for the processing of personal data.
Bribery Act 2010	2010	UK	Makes it illegal to bribe anyone, anywhere in the world.
Foreign Corrupt Practices Act (FCPA)	1977	US	Anti-bribery provision makes it unlawful for a US citizen, and certain foreign issuers of securities, to make a corrupt payment to a foreign official.
Sarbanes–Oxley Act (SOX)	2002	US	US Public Company Accounting Reform and Investor Protection Act.
Gramm-Leach-Bliley Act (GLBA)		US	Protects financial data.
Prevention of Corruption Act, 1988 (POCA)	1988	India	Criminalises bribery and other forms of corruption.
Companies Act, 2013 (CA)	2013	India	Sets out standards for corporate governance and financial reporting.

8.3 Critical National Infrastructure Compliance

Critical National Infrastructure (CNI) is defined as the assets, systems, sites, information, people, and processes that are essential for the functioning of a country and upon which daily life depends. It includes a wide range of sectors, such as energy, transport, water, communication, and healthcare.

Compliance with CNI regulations is essential to protect these critical sectors from cyberattacks and other threats. CNI operators must comply with the relevant regulations in order to protect their critical assets and systems from cyberattacks. Failure to comply with the regulations can result in significant fines and other penalties.

To remain compliant with the relevant regulations CNI operators should:

- Implement a comprehensive cybersecurity programme that includes policies and procedures to manage cybersecurity risks.
- Conduct regular risk assessments to identify and mitigate cybersecurity risks.
- Train employees on cybersecurity best practices.
- Use strong authentication and encryption to protect data and systems.
- Regularly patch and update systems and software.
- Have a plan in place to respond to cyberattacks.

8.3.1 The EU

The EU has enacted a suite of laws to meet the problem head on. In 2016 ***Directive (EU) 2016/1148, Network and Information Security (NIS)*** [47] was enacted. This established measures for a high common level of security of network and information systems across the Union. It came into force on 9 May 2018 and has been implemented by all member states. The NIS Directive applies to two categories of organisations:

- **Operators of Essential Services (OES)**: These are organisations that provide essential services to society, such as energy, transport, water, and healthcare. OESs are required to implement appropriate technical and organisational measures to manage the risks to their NIS.
- **Digital Service Providers (DSP)**: These are organisations that provide online services to consumers, such as social media platforms, online marketplaces, and cloud computing providers. DSPs are required to notify the competent authorities of any incidents that have a significant impact on the provision of their services or on the security of their users' data.

The NIS Directive also establishes a number of other requirements, including:

- Member States must designate National Competent Authorities (NCA) to oversee the implementation of the Directive and to coordinate their response to cybersecurity incidents.
- These NCAs must establish Computer Security Incident Response Teams (CSIRT) to help organisations respond to cybersecurity incidents.
- Member States must cooperate with each other and with the European Commission to share information about cybersecurity threats and incidents.

The NIS Directive has been credited with raising the level of cybersecurity awareness and preparedness among organisations in the EU.

8.3.1.1 Network and Information Security (NIS2)

Directive (EU) 2022/2555, Network and Information Security (NIS2) [48]. Measures to ensure a high common level of cybersecurity in the Union and amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972 and repealing the Directive (EU) 2016/1148 (NIS). This directive expands the scope of the previous directive to include more organisations, such as small and SMEs and public administrations. It also introduces new requirements for organisations, such as incident reporting and risk management. Some of the key changes introduced by NIS2 include:

- **Expanded scope**: NIS2 now applies to a wider range of organisations, including SMEs, public administrations, and certain digital service providers.
- **New requirements**: NIS2 introduces new requirements for organisations, such as incident reporting, risk management, and cybersecurity awareness training.
- **Increased enforcement**: NIS2 gives national authorities more powers to enforce the directive, including the power to impose fines of up to €10 million or 2% of global annual turnover for serious violations.

NIS2 is a significant step forward in the EU's efforts to improve cybersecurity. It is expected to help organisations to better protect themselves from cyber threats and to reduce the impact of cyber incidents. Here are some of the key benefits of the NIS2 Directive:

- It helps to improve the overall cybersecurity of NIS in the EU.
- It makes it easier for organisations to manage their cybersecurity risks.
- It reduces the number of cyber incidents.
- It promotes innovation in the cybersecurity sector.
- It helps to strengthen the EU's cybersecurity resilience.

8.3.2 The UK

Additionally, the UK transposed the EU NIS regulations into UK law as the ***Network and Information Systems Regulations 2018*** [49] and these provide legal measures to boost the level of security, both cyber and physical resilience, of network and information systems for the provision of essential services and digital services. The UK are currently examining these to provide greater security; however, they will not transpose the EU NIS2 regulations.

8.3.3 The US

In the US, there are a number of regulations in place to govern CNI security and . The the Cybersecurity and Infrastructure Security Agency (CISA) is responsible for coordinating the protection of CNI in the USA.

The main CNI regulations in the USA are the ***Cybersecurity Information Sharing Act of 2015*** [50] requires CNI owners and operators to develop and implement a cybersecurity plan and it allows private companies to share cyber threat information with the Department of Homeland Security (DHS) and other federal agencies and also enables the government to share cyber threat information with private companies.

Additionally, the ***Federal Information Security Modernization Act (FISMA) of 2014*** [51] requires federal agencies to implement appropriate security measures to protect their information systems.

8.3.4 India

Compliance with CNI regulations is essential to protect these critical sectors from cyberattacks and other threats. In India, there are a number of regulations in place to govern CNI security. The main CNI regulations in India are the ***Information Technology Act, 2000*** [17] which requires all organisations that collect, process, or store sensitive personal data or information to implement appropriate security measures to protect that data. The ***Information Technology (IT) (Amendment) Act, 2008*** [52] established the National Critical Information Infrastructure Protection Centre (NCIIPC), which is responsible for coordinating the protection of CNI in India and the ***National Information Security Strategy, 2020*** [22] sets out the government's strategy for information security in India.

8.3.5 CNI Summary

Table 5 outlines key regulations and policies from different countries and regions focused on cybersecurity and the protection of critical infrastructure.

Table 5: CNI Summary

Document	Year	Body	Specific Purpose
Directive (EU) 2016/1148, Network and Information Security (NIS)	2016	EU	To improve the overall level of cybersecurity within the EU by requiring operators of essential services and digital service providers to manage cybersecurity risks.
Directive (EU) 2022/2555, Network and Information Security (NIS2)	2022	EU	To update and strengthen the NIS Directive by expanding the scope of entities covered, introducing new requirements for risk management and incident reporting, and increasing the enforcement powers of supervisory authorities.
Network and Information Systems Regulations	2018	UK	UK implementation of the EU NIS.
Cybersecurity Information Sharing Act	2015	US	Requires CNI owners and operators to develop and implement a cybersecurity plan.
Federal Information Security Modernization Act (FISMA)	2014	US	Requires federal agencies to implement appropriate security measures to protect their IT.
Indian National Cyber Security Policy	2013	India	Provides a framework for protecting India's critical infrastructure from cyberattacks.
Information Technology (IT) (Amendment) Act, 2008	2014	India	Establishes the National Critical Information Infrastructure Protection Centre (NCIIPC), which is responsible for coordinating the protection of CNI.

8.4 Compliance Auditing

A compliance audit is an evaluation of an organisation, its systems and process to ascertain the validity and reliability of information and to provide an assessment of an organisations internal controls against compliance to the rules of business in the various acts applied to such business. The audit is carred out by an approved third party auditor who will compare the stated policies with the actual controls in place.

Continous auditing is an automated method of auditing by use of software program's to perform the audit on a continous basis replacing the periodic manual audit associated with the use of an auditor.

8.5 Business Ethics

Business or corporate ethics is a form of applied ethics that examines ethical principles and moral or ethical problems that arise in a business environment. It applies to all aspects of business conduct and is relevant to the conduct of individuals and business organisations as a whole. The range and quantity of business ethical issues reflects the degree to which business is perceived to be at odds with non-economic social values.

Many companies have formulated internal policies pertaining to the ethical conduct of employees. These policies can be broad language or they can be more detailed policies, containing specific behavioural ethics codes. They are generally meant to identify the company's expectations of workers and to offer guidance on handling some of the more common ethical problems that might arise in the course of doing business. It is hoped that having such a policy will lead to greater ethical awareness, consistency in application, and the avoidance of ethical disasters.

An increasing number of companies also requires employees to attend seminars regarding business conduct, which often include discussion of the company's policies, specific case studies, and legal requirements. Some companies even require their employees to sign agreements stating that they will abide by the company's rules of conduct.

9 Bibliography

[1] *European Treaty Series - No. 185 - Convention on Cybercrime*. 2001.

[2] Directive 2002/58/EC, *EU Privacy and Electronic Communications directive*. 2002. Accessed: Sept. 20, 2023. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:02002L0058-20091219

[3] Regulation (EU) 2016/679, *EU General Data Protection Regulation*, vol. Regulation (EU) 2016/679. Accessed: Oct. 20, 2023. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&qid=1696059781017

[4] Regulation (EU) 2019/881, *EU Cybersecurity Act*. 2019, p. 55. Accessed: Oct. 09, 2023. [Online]. Available: https://eur-lex.europa.eu/eli/reg/2019/881/oj

[5] Regulation (EU) 2024/2847, *EU Cyber Resilience Act (CRA)*. 2024. Accessed: June 13, 2025. [Online]. Available: https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng

[6] Regulation (EU) 2022/2554, *EU Digital Operational Resilience Act (DORA)*. 2022, p. 55. Accessed: Oct. 09, 2023. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R2554

[7] UK, *UK Computer Misuse Act 1990*. 1990. Accessed: Sept. 30, 2023. [Online]. Available: https://www.legislation.gov.uk/ukpga/1990/18/contents

[8] UK, *UK Data Protection Act 2018*. 2018. Accessed: Sept. 30, 2023. [Online]. Available: https://www.legislation.gov.uk/ukpga/1990/18/contents

[9] UK, *UK Investigatory Powers Act (IPA) 2016*. 2016. Accessed: Sept. 30, 2023. [Online]. Available: https://www.legislation.gov.uk/ukpga/2016/25/introduction

[10] UK, *UK Fraud Act 2006*. 2006. Accessed: Sept. 30, 2023. [Online]. Available: https://www.legislation.gov.uk/ukpga/2006/35/introduction

[11] USA, *US Export Administration Regulations (EAR)*. Accessed: Sept. 30, 2023. [Online]. Available: https://www.bis.doc.gov/index.php/regulations/export-administration-regulations-ear

[12] USA, *US Computer Fraud and Abuse Act (CFAA) 1986*. 1986. Accessed: Sept. 30, 2023. [Online]. Available: https://www.justice.gov/jm/jm-9-48000-computer-fraud

[13] USA, *US Economic Espionage Act (EEA) 1996*. 1996. Accessed: Sept. 30, 2023. [Online]. Available: https://www.justice.gov/archives/jm/criminal-resource-manual-1122-introduction-economic-espionage-act

[14] USA, *US Identity Theft and Assumption Deterrence Act (ITADA) 1998*. 1998. Accessed: Sept. 30, 2023. [Online]. Available: https://www.justice.gov/criminal-fraud/identity-theft/identity-theft-and-identity-fraud

[15] USA, *US Gramm-Leach-Bliley Act (GLBA) (Financial Services Modernization Act) 1999*. 1999. Accessed: Sept. 30, 2023. [Online]. Available: https://www.ftc.gov/legal-library/browse/statutes/gramm-leach-bliley-act

[16] USA, *US Health Insurance Portability and Accountability Act (HIPAA) 1996*. 1996. Accessed: Sept. 30, 2023. [Online]. Available: https://www.cdc.gov/phlp/publications/topic/hipaa.html

[17] India, *Indian Information Technology Act, 2000*. 2000. Accessed: Sept. 30, 2023. [Online]. Available: https://www.indiacode.nic.in/bitstream/123456789/13116/1/it_act_2000_updated.pdf

[18] India, *Indian Penal Code, 1860*. 1869. Accessed: Sept. 30, 2023. [Online]. Available: https://www.indiacode.nic.in/handle/123456789/2263?sam_handle=123456789/1362

[19] India, *Indian Information Technology (Amendment) Act, 2008*. 2009. Accessed: Sept. 30, 2023. [Online]. Available: https://www.indiacode.nic.in/bitstream/123456789/15386/1/it_amendment_act2008.pdf

[20] India, *Indian Information Technology Rules, 2011*. 2011. Accessed: Sept. 30, 2023. [Online]. Available: https://www.indiacode.nic.in/handle/123456789/1362/simple-search?query=The%20Information%20Technology%20(Reasonable%20Security%20Practices%20and%20Procedures%20and%20Sensitive%20Personal%20Data%20or%20Information)%20Rules,%202011.&searchradio=rules

[21] India, *Indian Indian National Cyber Security Policy, 2013*. 2013. Accessed: Sept. 30, 2023. [Online]. Available: https://www.meity.gov.in/writereaddata/files/National_cyber_security_policy-2013_0.pdf

[22] India, *Indian National Cyber Security Strategy, 2020*. 2020. Accessed: Sept. 30, 2023. [Online]. Available: https://www.meity.gov.in/writereaddata/files/National_cyber_security_policy-2013_0.pdf

[23] *Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies*. 1995. Accessed: Sept. 30, 2023. [Online]. Available:

https://www.wassenaar.org/app/uploads/2019/12/WA-DOC-19-Public-Docs-Vol-I-Founding-Documents.pdf
[24] Regulation (EC) No 428/2009, *EU regime for the control of exports, transfer, brokering and transit of dual-use items*. 2009. Accessed: Aug. 08, 2022. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32009R0428
[25] Regulation (EU) 2018/1922, *EU regime for the control of exports, transfer, brokering and transit of dual-use items*. 10/102018. Accessed: Oct. 09, 2023. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32009R0428
[26] UK, *UK Export Control (Amendment) (EU Exit) Regulations 2020*. S.I.: TSO, 2020. Accessed: Oct. 02, 2023. [Online]. Available: https://www.legislation.gov.uk/ukdsi/2020/9780348213782/introduction
[27] India, *Indian Foreign Trade (Development & Regulation) Act*. 1992. Accessed: Sept. 30, 2023. [Online]. Available: https://www.indiacode.nic.in/handle/123456789/1947?locale=hi
[28] EU Directive 95/46/EC, *EU protection of individuals with regard to the processing of personal data and on the free movement of such data*. 1995. Accessed: Mar. 10, 2003. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:31995L0046
[29] Regulation (EU) 2016/679, *EU General Data Protection Regulation (GDPR)*. 2016. Accessed: Mar. 10, 2020. [Online]. Available: https://eur-lex.europa.eu/eli/reg/2016/679/oj
[30] USA, *US California Consumer Privacy Act (CCPA) 2018*. 2018. Accessed: Sept. 30, 2023. [Online]. Available: https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375
[31] USA, *US Virginia Consumer Data Protection Act (VCDPA) 2023*. 2023. Accessed: Sept. 30, 2023. [Online]. Available: https://law.lis.virginia.gov/vacodefull/title59.1/chapter53/
[32] USA, *US Fair Credit Reporting Act (FCRA) 1970*. 1970. Accessed: Sept. 30, 2023. [Online]. Available: https://www.ftc.gov/legal-library/browse/statutes/fair-credit-reporting-act
[33] USA, *US Children's Online Privacy Protection Act (COPPA) 1998*. 1998. Accessed: Sept. 30, 2023. [Online]. Available: https://www.ftc.gov/legal-library/browse/rules/childrens-online-privacy-protection-rule-coppa
[34] USA, *US American Data Privacy and Protection Act (ADPPA), 2022 (Not passed into law)*. 2022. Accessed: Sept. 30, 2023. [Online]. Available: https://www.congress.gov/bill/117th-congress/house-bill/8152
[35] India, *Indian Digital Personal Data Protection Bill, 2023*. 2023. Accessed: Sept. 30, 2023. [Online]. Available: https://prsindia.org/billtrack/digital-personal-data-protection-bill-2023
[36] P. Cichonski, T. Millar, T. Grance, and K. Scarfone, 'NIST SP 800-61 Computer Security Incident Handling Guide', National Institute of Standards and Technology, NIST SP 800-61 Rev. 2, Jan. 2020. Accessed: Aug. 08, 2023. [Online]. Available: https://doi.org/10.6028/NIST.SP.800-61r2
[37] M. West-Brown, D. Stikvoort, Klaus-Peter Kossakowski, G. Killcrece, R. M. Ruefle, and M. T. Zajicek, 'Handbook for Computer Security Incident Response Teams (CSIRTs)', p. 1673727 Bytes, 2003, doi: 10.1184/R1/6574055.V1.
[38] Directive (EU) 2006/43/EC, *EU Audit Directive*. 2006. Accessed: Oct. 09, 2023. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32006L0043
[39] Regulation (EU) No 596/2014, *EU Market Abuse (market abuse regulation)*. 2014. Accessed: Oct. 09, 2023. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32014R0596&qid=1696372229904
[40] UK, *UK Bribery Act 2010*. 2010. Accessed: Sept. 30, 2023. [Online]. Available: https://www.legislation.gov.uk/ukpga/2010/23/introduction
[41] USA, *US Foreign Corrupt Practices Act (FCPA) 1977*. 1977. Accessed: Sept. 30, 2023. [Online]. Available: https://www.justice.gov/criminal-fraud/foreign-corrupt-practices-act
[42] USA, *US US Sarbanes–Oxley Act (SOX) 2002*. 2002. Accessed: Sept. 30, 2023. [Online]. Available: https://www.govinfo.gov/content/pkg/PLAW-107publ204/pdf/PLAW-107publ204.pdf
[43] India, *Indian Prevention of Corruption Act (POCA) 1988*. 1988. Accessed: Sept. 30, 2023. [Online]. Available: https://www.indiacode.nic.in/bitstream/123456789/1558/1/A1988-49.pdf
[44] India, *Indian Companies Act (CA) 2013*. 2013. Accessed: Sept. 30, 2023. [Online]. Available: https://www.indiacode.nic.in/handle/123456789/2114?sam_handle=123456789/1362
[45] 'Basel II Accord'. June 2004.
[46] *Basel III*, June 01, 2011. Accessed: Oct. 03, 2023. [Online]. Available: https://www.bis.org/publ/bcbs189.htm
[47] Directive (EU) 2016/1148, *EU Measures for a high common level of security of network and information systems across the Union*. 2016, p. 30. Accessed: June 09, 2023. [Online]. Available: https://eur-lex.europa.eu/eli/dir/2016/1148/oj

[48] Directive (EU) 2022/2555, *EU Measures to ensure a high common level of cybersecurity in the Union and amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972 and repealing the Directive (EU) 2016/1148 (NIS 2 Directive)*. 2022, p. 73. Accessed: Aug. 08, 2022. [Online]. Available: https://eur-lex.europa.eu/eli/dir/2022/2555/oj

[49] UK, *UK Network and Information Systems Regulations 2018*. 2018. Accessed: Sept. 30, 2023. [Online]. Available: https://www.legislation.gov.uk/uksi/2018/506/introduction

[50] USA, *US Cybersecurity Information Sharing Act 2015*. 2015. Accessed: Sept. 30, 2023. [Online]. Available: https://www.justice.gov/archives/jm/criminal-resource-manual-1122-introduction-economic-espionage-act

[51] USA, *US Federal Information Security Modernization Act (FISMA)*. 2014. Accessed: Sept. 30, 2023. [Online]. Available: https://www.congress.gov/bill/113th-congress/senate-bill/2521

[52] India, *Indian Information Technology (Ammended) Act, 2008*. 2009. Accessed: Sept. 30, 2023. [Online]. Available: https://www.indiacode.nic.in/bitstream/123456789/15386/1/it_amendment_act2008.pdf

This page is intentionally blank