Legal Responsibilities 1

As cybersecurity is such a major concern in the modern world, there have been several laws implemented to help protect against these threats. These have been revised and amended over time to ensure they reflect the threats that affect us today.

In this lesson, we'll learn about two major pieces of legislation that have had a big impact on cybersecurity, and the amendments that have changed them. These are the:

1. Data Protection Act (1998)
2. Computer Misuse Act (1990)

1. Data Protection Act (1998)

The Data Protection Act was introduced in 1998 to protect the privacy of individuals by ensuring that their personal information is processed in an ethical manner.

This doesn't just cover digital data stored on a computer. It covers data stored on paper and even audio data. However, it has become much more relevant due to the ease in which information is shared thanks to IT systems.

The Information Commissioners Office (ICO) is an independent body who is responsible for investigating possible data protection violations. If it is found that a business has been in breach of the Data Protection Act (1998) then they could be given a fine of up to £500,000.

General Data Protection Regulations

On the May 25th, 2018 an EU law called the General Data Protection Regulations (GDPR) became enforced in all EU member states.

The General Data Protection Regulations replaced the Data Protection Act (1998) along with another EU law called the Data Protection Directive.

It made a number of changes to the DPA (1998), though much is largely similar. For example, in the table below are summarised the principles of both the previous and current law.

Data Protection Act (1998)	General Data Protection Regulations
1 – Personal data shall be processed fairly and lawfully.	(a) – Personal data shall be processed lawfully, fairly and in a transparent manner in relation to individuals.
2 – Personal data shall be obtained only for one or more specified & lawful purposes.	(b) – Personal data shall be collected for specified, explicit and legitimate purposes.
3 – Personal data shall be adequate, relevant and not excessive.	(c) – Personal data shall be adequate, relevant and limited to what is necessary.
4 – Personal data shall be accurate and, where necessary, kept up to date.	(d) – Personal data shall be accurate and, where necessary, kept up to date.
5 – Personal data shall not be kept for longer than is necessary for its purposes.	(e) – Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary.
6 – Personal data shall be processed in accordance with the rights of data subjects under this Act.	No principle, however separate provisions are made that expand on this principle.
7 – Appropriate technical and organisational measures shall be taken to protect data.	(f) – Personal data shall be processed in a manner that ensures appropriate security of the personal data.

8 – Personal data shall not be transferred to a country or territory outside the EEA without adequate protection.	No principle, however separate provisions are made that expand on this principle.

There was an additional, separate, principle added known as the accountability principle. This requires that you must have appropriate measures and records in place to be able to demonstrate your compliance with the GDPR.

The two principles missing from the General Data Protection Regulations have been expanded greatly into their own sections of the law.

In particular, the rights of the data subject have been expanded and defined many individual rights, such as the right to access, rectification, erasure & to individual decision making.

Other changes include that the requirement of appointing a Data Protection Officer in an organisation, given certain conditions, as well as the requirement to inform the ICO of any data breaches within 72 hours of discovery.

Finally, the fine for failing to meet data protection requirements was increased significantly. The maximum fine is now €20 million or 4% of a business's annual turnover, whichever is largest.

In the UK the GDPR was implemented as the Data Protection Act (2018) in preparation for the withdrawal from the EU.

Further Thought

Research into each of these data protection principles and what must be done to meet the requirements for each of them.

2. Computer Misuse Act (1990)

The Computer Misuse Act was brought into force in 1990 to protect users against the theft and damage of the information they store using IT systems. Before this point many cybersecurity offences, including hacking, were not actually illegal.

Broadly speaking, this legislation covers hacking and spreading viruses. You can even be punished for attempted hacking, even if not successful. You also don't need to have malicious intent, if you gain unauthorised access to a system but do nothing, you can still be punished.

The three original crimes that were covered by this act:

- **Offence 1** – Unauthorised access to computer material. This is covering the hacking of a computer system. This can be punished by up to 2 years in prison and/or a large fine.
- **Offence 2** – Unauthorised access with intent to commit or facilitate commission of further offences. This could be using the data obtained by hacking to blackmail someone. This can be punished by up to 5 years in prison and/or a large fine.
- **Offence 3** – Unauthorised acts with intent to impair, or with recklessness as to impairing, operation of a computer. This could be altering the data found when hacking a system, or spreading a virus which damages data. This can be punished by up to 10 years in prison and/or a large fine.

Police and Justice Act (Computer Misuse)

In 2006 the Police and Justice Act 2006 (Computer Misuse) extended the Computer Misuse Act.

It made modifications to Offence 1 so that the punishment increased to 2 years imprisonment (it was originally just six months). It also allowed offence 3 to cover Denial of Service attacks.

Finally, it added an additional offence to the Computer Misuse Act:

- **Offence 3a** – Making, supplying or obtaining anything which can be used in computer misuse offences. This could be creating a malware program, such as a virus or worm, that can be used to gain access to a system and/or harm data. This can be punished by up to 2 years in prison and/or a large fine.

Further Thought

The Computer Misuse Act was originally brought in after a very high-profile hack of the Royal Mail Prestel system. It was found that the two hackers involved couldn't be punished as no legislation adequately covered the crime. Research about this hack and what followed online.

Lesson Summary

- The Data Protection Act (1998) protects the privacy of individuals by ensuring that their personal information is processed in an ethical manner. There are 8 principles that must be complied with. If in breach of the DPA then an organisation can be fined as much as £500,000.
- The General Data Protection Regulations were enforced in the UK under a new law called the Data Protection Act (2018).
- This new data protection law made changes to the principles, expanding the requirements on organisations handling personal data, and increased the punishment to €20 million or 4% of a business's annual turnover, whichever is largest.
- The Computer Misuse Act (1990) protects users against the theft and damage of the information they store using IT systems. There are different punishments depending on the crime but could be as much as 10 years in jail and/or a large fine.
- The Police and Justice Act 2006 (Computer Misuse) extended the Computer Misuse Act so that it covered Denial of Service Attacks as well as the making, supplying or obtaining anything which can be used in computer misuse offences.

Legal Responsibilities 2

Last lesson we looked at two key laws that directly relate to making cybersecurity attacks illegal. There are several other laws that relate to cybersecurity though, whether by giving organisations rights to protect themselves or through making cybersecurity related activities illegal.

In this lesson, we'll learn about some of these related legislation and the amendments that have changed them, including:

1. Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations (2000)
2. Fraud Act (2006)
3. Health & Safety at Work Act (1974)

1. Telecommunications Regulations (2000)

Individuals, including employees of a business, have a right to privacy. This is protected under the Human Rights Act (1998).

However, organisations need to be able to monitor communications over their network in order to protect itself from cybersecurity threats. They are given the legal right to do so under the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations (2000).

Without this piece of legislation, an organisation would only be able to monitor communications with the consent of both the sender and receiver of the communication. This would be extremely ineffective as no cyber attacker would give their consent.

However, now this law is in place organisations can monitor communications on their private network as long it is for one of a set number of purposes. These are:

- To establish the existence of facts and ascertain compliance with regulations & that a person is performing their duties.

- In the interests of national security
- To prevent or detect crime
- To investigate or detect unauthorised use of the network
- To secure and ensure the effective operation of the network

This monitoring does need to be done with respect to the Human Rights Act and Data Protection Act, so businesses must be cautious and appropriate with their monitoring.

Further Thought

The ICO has published codes of practice on the monitoring of employees at work. Research these codes of practice online and how they might limit the organisation's security if complied with.

2. Fraud Act (2006)

The Fraud Act (2006) replaced the offences relating to deception from the Theft Act (1978). This previous Theft Act was criticised for its complexity, including difficulties of choosing which fraud offence to proceed with which lead to many criminals escaping punishment.

The Fraud Act, thankfully, simplified the act of fraud to make trying this crime much more achievable.

The offences can be split into three classes. These are:

- Fraud by false representation
- Fraud by failing to disclose information
- Fraud by abuse of power.

For all of these though, the offender must have acted dishonestly with the intent of making a gain or cause a loss (or risk of loss) on another. It's worth noting that no gain or loss needs to actually have been made, the attempt, even if not successful, is enough.

The punishment if found guilty of this crime is up to 10 years imprisonment.

Obviously, this legislation is not just about cybercrime but covers all kinds of fraud. However much of cybercrime does relate to fraud, such as using spyware or hacking to access bank details to then steal money from their account (bank fraud).

Further Thought

Section 11 of the Fraud Act (2006) refers to “obtaining services dishonestly”. How does this relate to cybercrime?

3. Health & Safety at Work Act (1974)

This is the primary legislation for ensuring the health, safety and welfare of individuals at work. Employers must do whatever is practicable to ensure this.

Employers must perform a risk assessment to identify all risks that may cause harm to an employee in the workplace. There are also a number of specific duties they must perform, including:

- Provide a safe system of work
- Provide arrangements for ensuring safe handling, storage and transport of articles and substances
- Provide information, instruction, training and supervision to employees of risks
- Maintain the workplace in a condition that is safe & without risks
- Provide and maintain a work environment that is without risk to health and provide facilities and arrangements to ensure employee welfare
- Provide a health & safety policy
- Consult with employees, or elected representative, over risks.

Employees also have a duty under the Health & Safety at Work Act. They must take care of their own health & safety and that of others that may be affected by their actions. They must also bring any queries or concerns to their employer.

The Health & Safety at Work Act is enforced by the Health & Safety Executive. If found guilty of an HSWA offence, then you can receive an unlimited fine. There is also a possibility of a

prison term in some cases. This can be as much as 2 years imprisonment. Finally, you could also be liable to compensation to be paid to the victims of the offence.

It is possible that the HSE could place prohibitions on a business that will ban certain activities that have been identified as being a risk of causing serious personal injury.

Further Thought

The Health and Safety (Display Screen Equipment) Regulations 1992 add specific responsibilities of employers to employees that use display screen equipment in the workplace. What are these?

Lesson Summary

- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations (2000) allow businesses to monitor employees use of the company network.
- This is important in ensuring businesses to detect and prevent cyber security attacks on their business.
- The Fraud Act (2006) simplified previous legislation on fraud. It makes fraud by false representation, by failing to disclose information or by abuse of power illegal with a maximum 10 years imprisonment.
- As the goal of many cybercrime attacks is for the purpose of bank and identity fraud, this helps to deter potential attackers.
- The Health & Safety at Work Act (1974) placed responsibilities on employers and employees in ensuring that a workplace is a safe place.
- The HSE enforce this law and punishments can be an unlimited fine and even a 2-year prison sentence. The HSE can also place prohibitions on a business to stop them from performing certain activities.