The Importance of Cyber-Security

By Laura Morgan: Joint Examiner - Professional 2 Audit Practice.

Today, there is a significant increase in cybercrime due to the reliance on technology in all aspects of life. In 2018, the number of cyber-attacks in Ireland doubled from the previous year. I believe the following quotes by the National Cyber Security Centre (NSCS) highlight the importance of cyber-security in today's society:

- *"Cyber risk is now one of the most commonly talked about topics as the impact of cybercrimes reaches an all-time high."*
- *"This is big, global business and cyber threats will therefore continue to multiply and evolve rapidly."*
- *"No industry has been spared, with high impact attacks reported across a broad range of sectors."*

It is vital that all businesses today, invest in cyber-security in order to protect themselves and their customers. The impact of cybercrime on an organisation and the measures they have in place, is a topic which is becoming increasingly more relevant on each external audit.

What is cyber-security?

Cyber-security is the practice of protecting systems, networks and programs from digital attacks.

These cyber-attacks are usually aimed at:

- Accessing, changing or destroying sensitive information;
- Extorting money from users; or
- Interrupting normal business processes.

Types of cyber-attacks

There are a number of different types of cyber-attacks as detailed below:

1. **Ransomware** – One of the fastest-growing forms of cyber-attack, ransomware is a type of malware that demands payment after encrypting the victim's files, making them inaccessible. Paying the ransom does not guarantee the recovery of all encrypted data.

2. **Malware** – Malware is a broad term used to describe any file or programme intended to harm a computer – e.g. a virus

3. **Social engineering** – Social engineering is used to deceive and manipulate victims to gain computer access. This is achieved by tricking users into clicking malicious links or by physically gaining access to a computer through deception.

4. **Phishing** – Phishing attacks are continually on the rise. Often indistinguishable from genuine emails, text messages or phone calls, these scams can inflict enormous damage to organisations.

Why is cyber-security so important today?

- This is an extremely important topic for management in all organisations, due to the increase in regulations and reporting requirements.
- In May 2018, the EU introduced GDPR (General Data Protection Regulation), and now organisations can be faced with fines up to 20 million euro or 4% of annual global turnover for non-compliance with the regulations.
- As most people in today's society rely on technology in all aspects of life (laptop, iPad, iPhone), there sometimes can be a fine line between work and their personal life, which significantly increases their vulnerability to a cyber-attack.
- As cyber-attacks are becoming increasingly sophisticated, it is important that organisations have appropriate IT security in place.
- Although the technology is extremely important in preventing a cyber-attack, it is vital that staff have received training in order to be aware of the processes to be implemented, and how to identify when they are coming under threat.
- If an organisation does not have appropriate measures in place, they may also suffer non-financial costs such as damage to their reputation and loss of trade.

One of the biggest cyber attacks in recent times, was the attack on the UK's National Health Service (NHS) in May 2017. Following the ransomware attack, over 40 NHS Trusts and hospitals were unable to serve their patients. IT systems were largely affected, including the diversions of ambulances and hackers also accessed thousands of patient records, including reports of blood tests, medicines and patient histories. The cyber-attack happened as a result of the NHS using outdated IT systems. This was declared a "major incident" by the NHS, and was among the biggest cyber-attack of its kind in history.

In addition, in November 2016, Tesco suffered a major embarrassment after fraudsters succeeded in withdrawing money from 20,000 of the bank's 136,000 current accounts – a total of £2.5 million. Suspicious activity was also observed across 40,000 accounts belonging to their customers. The chief executive of the FCA termed the bank fraud as 'extremely serious'. Tesco was fined £16.4 million as a result of the attack.

The attacks above happened before GDPR was introduced, so the fines imposed were not as heavy as they would be now.

Cyber-security – Audit considerations

In accordance with *ISA 315, 'Identifying and assessing the risks of material misstatement through understanding the entity and its environment'*, the auditor is required to carry out various risk assessment procedures in order to gain an understanding of the entity and its environment. In relation to cyber-security, it is important that the auditor considers the following factors:

- **Accounting systems and technology –** it is important that the entity is using appropriate accounting systems and technology that is up to date and can reduce the risk of cyber-crime.
- **General IT controls** – it is important that the organisation is able to restrict access to sensitive information by unauthorised individuals. The auditor will check the IT controls the organisation has in place (such as usernames, passwords, how often the passwords are reset) to ensure they are appropriate.
- **Data Protection –** the auditor should assess how the organisation protects the data it holds (this may be increasingly important where the entity has online sales). It is important that the organisation complies with GDPR.

It is important that the auditor is made aware of any cyber attacks the organisation has faced, and if a breach of data protection has occurred. The auditor may be able to find out this information through management inquiries, a review of board minutes and media attention.

If a breach of data protection has occurred, the auditor will have to consider the financial implications of the breach and whether a provision has been recorded within the financial statements in accordance with IAS 37. In addition, depending on the extent of the breach, the auditor may have to consider if there is any impact on the going concern of the organisation in accordance with *ISA 570, Going Concern*.