Cyber security: business briefing

This business briefing highlights the key issues that a business needs to understand about cyber security.

What is a cyber attack?

A cyber attack is an assault by a third party via a computer against another computer or computer system, which is intended to compromise the integrity, availability or confidentiality of that computer or computer system. For example:

- A remote attack on a business's IT systems or website.
- Attacks on information held in third-party systems (for example, the company bank account).

Understanding the risks faced by the business

Identify what assets need to be protected

Every business should identify the key assets that need to be protected from a potential cyber attack. For example:

- Customer databases.
- Financial information.
- IT services (such as the ability to take payments via the company website).
- Intellectual property (such as product designs or manufacturing processes).
- IT equipment.
- Sensitive personal data.

Consider the impact that a cyber attack could have on the business

- **Financial loss.** Financial losses stemming from:
    - theft of information, bank details or money;

    - disruption to trading (especially if the business undertakes a lot of online transactions); or

    - costs associated with cleaning up affected systems and getting them functioning again.

- **Reputational damage.** A business that has been the victim of a cyber attack will be keen to convince its customers, owners, employees and the general public that the incident was a one-off event and the situation is now under control. Reputational damage can often lead to a reduction in profits and the erosion of a business's customer base.

- **Regulatory sanctions.** The business could be fined if personal data is lost or compromised due to a cyber attack. Data protection laws require businesses to implement appropriate technological and organisational security measures against unauthorised or unlawful processing, accidental loss and destruction or damage of personal data.

Planning for a potential cyber attack

Businesses should contact their suppliers, major customers and competitors to find out whether they have been the victim of a cyber attack. This information will help the business decide whether it may be the target of an attack.

Security controls

Consider instructing a third-party IT security consultant to determine whether the business's existing security processes provide sufficiently robust protection. A specialist consultant will also have experience of how other similar businesses are responding to the threat of a cyber attack.

Contractual commitments

Analyse the business's existing contractual commitments and requirements. A cyber attack can cause severe disruption to a business and it is important to understand the impact the attack may have on its contracts as, under English law, contractual obligations cannot easily be avoided.

Educating employees

- The business should produce a policy detailing how employees should use its systems in the most secure manner.

- Employees should be given appropriate internal training (both for new joiners and regular refreshers for existing employees) so that everyone understands their role in keeping the business secure.

- Businesses should put reporting processes in place to enable employees to raise concerns about other members of staff that they think are failing to comply with the policy.

Business continuity planning

- Produce a plan detailing who to contact for support if the business is attacked or its online services are disrupted. The plan should set out the business's recovery procedures and explain how it would continue operating, particularly if the business trades online.

- Important business records (for example, sales information) should be backed up regularly and archived in a secure, off-site location that can be easily accessed after a cyber attack.

- Compile hard copies of staff, supplier and customer contact lists. The business should ensure that copies are retained off site and kept secure, for use in the event of an attack.

Implementing measures to protect the business from a cyber attack

Businesses can take a number of steps to improve their security controls:

- **Malware protection.** Install anti-virus solutions on all systems and keep software and browsers up to date. Consider restricting access to inappropriate websites to reduce the risk of being exposed to malware (malicious software).

- **Network security.** Increase protection of the business's networks (including wireless networks) against external attacks through the use of firewalls, proxies and other measures.

- **Secure configuration.** Maintain an inventory of all IT equipment and software. Identify a secure standard configuration for all existing and future equipment used by the business.

- **Managing user privileges.** Restrict employee and third-party access to IT equipment, systems and information to the minimum required. Excessive user privileges, with too many employees having access to confidential information or systems that do not help them perform their job, should be avoided.

- **Home and mobile working.** Home and mobile working increases a company's cyber risk profile. A business should draft and implement a home and mobile working policy and train employees to adhere to it, especially if the business allows employees to use personal mobile devices (for example, laptops or tablets) for business use.

- **Removable media.** Restrict the use of removable media (such as USB drives). Make sure any data stored on removable media is protected to avoid the data being lost and to help prevent malware from being installed on the company's IT networks.

Ongoing security management issues

- Ensure that all IT systems and networks are continuously monitored against attack.

- Test, monitor and improve security controls on a regular basis.

- Remove any software or equipment that is no longer used, ensuring that any sensitive information stored on it is deleted before it is disposed of.

- Review and manage any change in user access, such as the creation of e-mail accounts when new employees arrive and the deletion of accounts when they leave.

Responding to a cyber attack

There are several actions that the business may need to consider taking following an attack, including:

- Addressing gaps in the business's security that have been identified due to the incident.
- Identifying and removing any ongoing threats (for example, malware).
- Reporting the incident to the police via the Action Fraud website.
- Establishing whether the business is obliged to notify regulators or other bodies of the attack.
- Notifying customers and suppliers if their data has been lost or compromised.

If you have any queries regarding this or any other matter please do not hesitate to contact Jamie Berry, Head of the Business Law Department at jamie.berry@twmsolicitors.com

Information contained in this article and on our website does not constitute legal advice and is provided for information purposes only. Recipients should not act upon it, but should seek legal advice relevant to their own situation.