Cyber security: how to protect your business

Sony was recently victim to a cyber-hacking incident so catastrophic that even the President of the United States of America stepped in. Whilst the hackers were never identified, what was certain was that they were smart and even the biggest, global companies were not safe. With the ever-changing nature of the internet, the likelihood of damaging security breaches online is increasing. In the UK in 2014, 81% of large organisations had experienced a security breach of some sort. This cost each organisation on average, between £600,000 and £1.5million. As a result, businesses around the world have realised the need to take proactive steps to increase protection for their cyber activities.

The UK's Department for Business, Innovation and Skills (BIS) developed the Cyber Essentials Scheme in 2014 which set out the basic controls that all organisations should implement to mitigate the risk from common internet based threats, within the context of the UK Government's 10 steps to Cyber Security. The Scheme also provides an Assurance Framework which offers a mechanism for organisations to demonstrate to customers, investors, insurers and others that they have taken these essential precautions.

The 10 steps, in summary, are as follows:

- Information risk management regime – assess the risks to your organisation's information assets and communicate your risk management policy across your organisation.
- Secure configuration – introduce policies and processes to develop secure baseline builds, and manage the configuration and use of your information and communication technology (ICT) systems.
- Network security – follow recognised network design principles when configuring perimeter and internal network segments, and ensure all network devices are configured to the secure business build.
- Managing user privileges – all users of your ICT systems should only be provided with the user privileges that they need to do their job. Control and monitor the number of people who are system or database administrators.
- User education and awareness – produce user security policies that describe acceptable and secure use of your organisation's ICT systems. These should be formally acknowledged in employment terms and conditions.
- Incident management – establish an incident response and disaster recovery capability that addresses the full range of incidents that can occur.
- Malware prevention – produce policies that directly address the business processes that are vulnerable to malware.
- Monitoring – establish a monitoring strategy and develop supporting policies.
- Removable media controls – produce removable media policies that control the use of removable media for the import and export of information.
- Home and mobile working – assess the risks to all types of mobile working and develop appropriate security policies.

The Cyber Essentials Scheme covers the basics of cyber security in an organisation's IT system. It concentrates on five key controls: (a) boundary firewalls and internet gateways, (b) secure configuration, (c) access control, (d) malware protection and (e) patch management.

The Assurance Framework is designed to provide a simple means for third parties to distinguish between organisations that are implementing basic cyber security controls from those that are not. There are two levels of certification, Cyber Essentials and Cyber Essentials plus. Organisations who receive a certificate will be able to display the appropriate badge.

If you are worried about the protections in place for your business, contact 3HR who will be able to advise you about the steps to take to ensure the security of your cyber activities.

Shamina Chowdhury
Solicitor
shamina.chowdhury@3hrinsurance.com