Q underwriting

Cyber Risk Management

What is "Cyber Risk"?

The Institute of Risk Managers (IRM) defines a cyber risk as any risk of financial loss, disruption, or damage to the reputation of an organisation from some sort of failure of its information technology systems.

Cyber risks can include:

- Theft and release of personal data, or stolen data being used for blackmail or extortion
- Falling prey to ransomware or denial of service attacks
- Damage to data by a computer virus or unintentionally transmitting a virus to a third party
- Direct theft of money from the organisation's account, or theft of customers' bank details
- Impersonation of the organisation to make purchases or set up credit agreements

plus a wide range of other scenarios.

Cyber Risk Management

There are some simple steps that you can follow to improve cyber security within your organisation:

Backups

Personal data is a valuable resource; consider how much you rely on your organisation's critical data such as client / supplier / process data, governing documents, payment and invoice records and more… All organisations should back up this important data; secure, offsite backups ensure you can operate following a major event such as a flood or fire and can make you more resilient to cybercrime.

Viruses and Malware

Protect your organisation from malicious software (malware, or viruses) by following these steps:

Install antivirus software (AV) and ensure the AV is on and automatically updates. Prevent users from downloading programs or suspicious files on your machines; users should only have permissions to do what is necessary in their role. Keep all equipment (hardware) and programs (software) up-to-date ('patching'). Prevent users from loading USBs or other peripherals. Install a firewall; this protects your internal network from external networks.

Devices

Mobile technology is essential to most organisations' operations and many people use mobile phones and tablets.

Ensure all devices have strict policies on password protection (and enforce the use of strong passwords where possible). Enable device tracking and remote wiping ('mobile device management'). Keep devices' operating systems (iOS, Android, etc.) up-to-date and install app updates when they become available. Don't use unknown WiFi hotspots, even if the vendor claims their WiFi is secure – everything transmitted could be intercepted; if possible, use your phone's hotspot for improved security.

Passwords

As above, ensure all devices, programs, files, etc. have strict policies on password protection; enforce the use of strong passwords where possible; force users to change passwords regularly; change all default passwords, such as those on WiFi routers. Use two-factor authentication where possible.

Phishing

Train staff about the risk of phishing attacks where scammers send faked or 'spoofed' emails containing fraudulent links trying to steal some information that can be used to later trick or scam you.

Summary

Directors must have a comprehensive awareness of Cyber Risks and consider what protections are necessary across all operational and administrative areas. You may also consider specialist cyber insurance.

Wherever possible seek expert advice.

Further information

Cyber Essentials

Q Underwriting Services Limited is authorised and regulated by the Financial Conduct Authority FRN 657367. Registered in England under No. 08946569. Registered office: Rossington's Business Park, West Carr Road, Retford, Nottinghamshire, DN22 7SW. 25/03/22 Ref: QD2128.1

Disclaimer: This information does not constitute any form of opinion or specific guidance, legal or financial advice and is for informational purposes only. The content is not intended to be a substitute for professional advice. We make no warranties as to the accuracy, reliability, or correctness of the information provided. You should seek specific, professional advice before taking any further action.