CLEAR
INSURANCE MANAGEMENT

Cyber Security Guide

Planning, Implementation and Review

Many small business owners have taken advantage of online business tools, such as advertising, carrying out financial transactions and communicating with customers and suppliers. However, this increase in usage also brings new and more complex risks into the equation. Every day throughout the United Kingdom, attacks on security and IT systems try to steal private information or disrupt businesses. According to a recent study by the Department for Business, Innovation and Skills, 87 per cent of small business respondents experienced a security breach within the past year.

Understanding Your Risks

As a small business owner, you need to protect your computer-based equipment, data and information from unauthorised access. While it is almost impossible to prevent all risks, the majority of risks can be prevented with basic security practices. It does not have to cost a lot of money, nor do you have to be an IT expert to implement these practices. Even by taking basic measures, you can protect your assets, reputation and customers and help your business thrive.

Common Types of Attacks

Cyber attacks typically target your business's information and IT-based services and equipment. Information commonly stolen includes client lists, transactions, databases, financial details, pricing information and personal data. This can occur through theft or unauthorised access of equipment, remote attacks on the IT system or your website, and attacks on information held on third-party systems, such as a cloud-based system.

Sources of the Attacks

Cyber attacks don't just come from outside parties (criminals and competitors) trying to steal from or disrupt your business—they can also come from current or former employees. Employees have access to privileged information and can compromise it by accident, through negligence or with malicious intent. Even leaving a laptop unattended for a few minutes can pose a threat.

Consequences of the Attacks

One single attack could seriously damage your business and can cause significant financial losses and costs. Financial losses may occur when financial and bank details are taken, everyday business is disrupted or even when business is lost due to a damaged reputation. A poor reputation can shrink your customer base. There are also significant costs involved with a successful cyber attack. Costs include cleaning up and restoring equipment, IT systems, networks and websites. The Information Commissioner's Office could fine you for noncompliance with the Data Protection Act. Attacks can also damage other companies you are associated with, such as suppliers or business partners.

Managing Your Risks

Managing your cyber risks can be accomplished in three simple steps: planning, implementation and review. The following pages provide principle assessment questions and a checklist for each step.

Step 1: **Planning**

Assessment Questions	1. What information assets are critical to your business? What kind of risks could they be exposed to?
	2. What legal and compliance requirements is your business subject to?
	3. How could you continue to do business if you were attacked? How could you manage these risks on an ongoing basis?

Planning Checklist

Make information security part of your normal business risk management procedures.

Consider whether your business could be a target for an attack. Ask your suppliers, major customers or similar businesses if they have been attacked, so you can learn from their experiences.	☐
Know whether you need to comply with personal data protection legislation, such as the Data Protection Act and Payment Card Industry compliance.	☐
Identify financial and information assets critical to your business. Identify essential IT services, such as online payment. Evaluate all IT equipment, including mobile and personal IT devices. Understand the risks to all of these things by considering how they are currently managed and stored, and who has access to them.	☐
Assess the level of password protection required to access equipment and online services by staff, third parties and customers. Determine whether more security is needed.	☐
Ensure all staff is properly trained and understands their role in cyber security.	☐
Decide whether additional investments or expert advice is needed to properly protect your business. If so, seek appropriate advice.	☐
Determine who can provide assistance if you are attacked or if online services are disrupted. Define recovery procedures and plan how to keep your business running in the event of an attack.	☐

Step 2: **Implementation**

Assessment Questions	1. Do you have the right security controls in place to protect your information, equipment, IT system and outsourced services?
	2. Does your staff know what their responsibilities are? Are they aware of best practices?
	3. How will you deal with an attack or threat? How will you get your business running again? Who can you turn to for assistance?

Implementation Checklist

Put the proper security controls in place for your business. If third-party IT services are used, check your contracts and service level agreements, and ensure that security controls are in place.

Install malware protection or anti-virus solutions on all systems and keep all software up to date. Restrict access to inappropriate websites. Create a security update policy detailing how and when updates are to be installed.	☐
Protect your networks, including wireless ones, with firewalls, proxies, access lists and other measures.	☐
Identify a standard secure configuration for all IT equipment. Maintain an inventory of all equipment and software. Change any default passwords.	☐
Manage user privileges and restrict access (staff and third-party) to the minimum required. Keep equipment physically secured to prevent unauthorised access.	☐
For home and mobile workers, ensure that sensitive data is encrypted when stored or transmitted online so that data can only be accessed by authorised users.	☐
Restrict the use of removable media such as USB drives, CDs, DVDs and secure digital cards. Protect any data stored on such media to prevent losing data and to prevent malware from being installed.	☐
Monitor use of all equipment and IT systems, collect activity logs and make sure you know how to identify unauthorised or malicious activity.	☐

Step 3: **Review**

Assessment Questions	1. Are you reviewing and testing the effectiveness of your control measures?
	2. Are you actively monitoring and acting on the information received?
	3. Are you keeping up with the latest cyber risks and threats?

Review Checklist

Periodically review your security and respond to any changes or problems you identify.

Test, monitor and improve your security controls on a regular basis to manage any changes to your level of risk.	☐
Remove any software or equipment that is no longer needed. This will ensure sensitive information stored on it will be disposed of.	☐
Review and manage changes to user access.	☐
If attacked, ensure that the response includes removing on-going threats (such as malware), understanding the cause of the incident and addressing any gaps in your security that were identified.	☐
Report online fraud and attack to the police via the Action Fraud website at www.actionfraud.police.uk/report_fraud. You may also need to notify customers and suppliers if their data has been compromised or lost.	☐