HM Government

Small businesses:
What you need to know about cyber security

Contents

Why you need to know about cyber security 3
Understanding the risks to your business 4
How you can manage the risks 5
Planning your cyber security 6
Implementing your cyber security 7
Reviewing your cyber security 8
Scenario: small business loses important contract 9
Where to get more information and advice 10

Why you need to know about cyber security

Cyber security is about protecting your computer-based equipment and information from unintended or unauthorised access, change or destruction.

Most of us now use the internet to do business, to advertise and sell, find new markets, customers and staff, communicate with customers and suppliers, and carry out our financial transactions. The internet brings huge opportunities and benefits. But it also brings risks. Every day there are attacks on the IT systems of UK companies like yours, attempting to steal your information and money or disrupt your business.

You can never be totally safe, but most online attacks can be prevented or detected with basic security practices for your people, processes and IT systems. These security practices are as important as locking your doors or putting your cash in a safe. You can manage your online security in the same way you would protect any other aspect of your business. With more customers demanding that their suppliers are secure, this is becoming a business necessity.

This guidance provides you with a good practice foundation for business owners and managers. You'll find links to other sources of good advice at the end of this booklet if you need them. You don't need to be an IT expert to improve your security. Taking some simple steps can help make all the difference.

Take the simple steps set out in this booklet and your business will benefit. You can save money through adopting an efficient risk management approach - plan, implement and review. You can gain a competitive advantage by being seen to take security seriously. Good security can be an enabler for a thriving business: you will be protecting your assets, your reputation, your customers, and your peace of mind.

Understanding the risks to your business

What is directly at risk?

Your money, your IT equipment, your IT-based services and your information. Information is an asset that can take many forms: client lists, customer databases, your financial details, your customers' financial details, deals you are making or considering, your pricing information, product designs or manufacturing processes. There is a risk to your IT services and information wherever they are stored, whether held on your own systems and devices, or on third-party hosted systems (the cloud).

Who could pose a threat to these assets?

- Current or former employees, or people you do business with. Compromising your information by accident, through negligence, or with malicious intent.
- Criminals. Out to steal from you, compromise your valuable information or disrupt your business because they don't like what you do.
- Business competitors. Wanting to gain an economic advantage.

What form could the threat take?

- Theft or unauthorised access of computers, laptops, tablets, mobiles.
- Remote attack on your IT systems or website.
- Attacks to information held in third party systems e.g. your hosted services or company bank account.
- Gaining access to information through your staff.

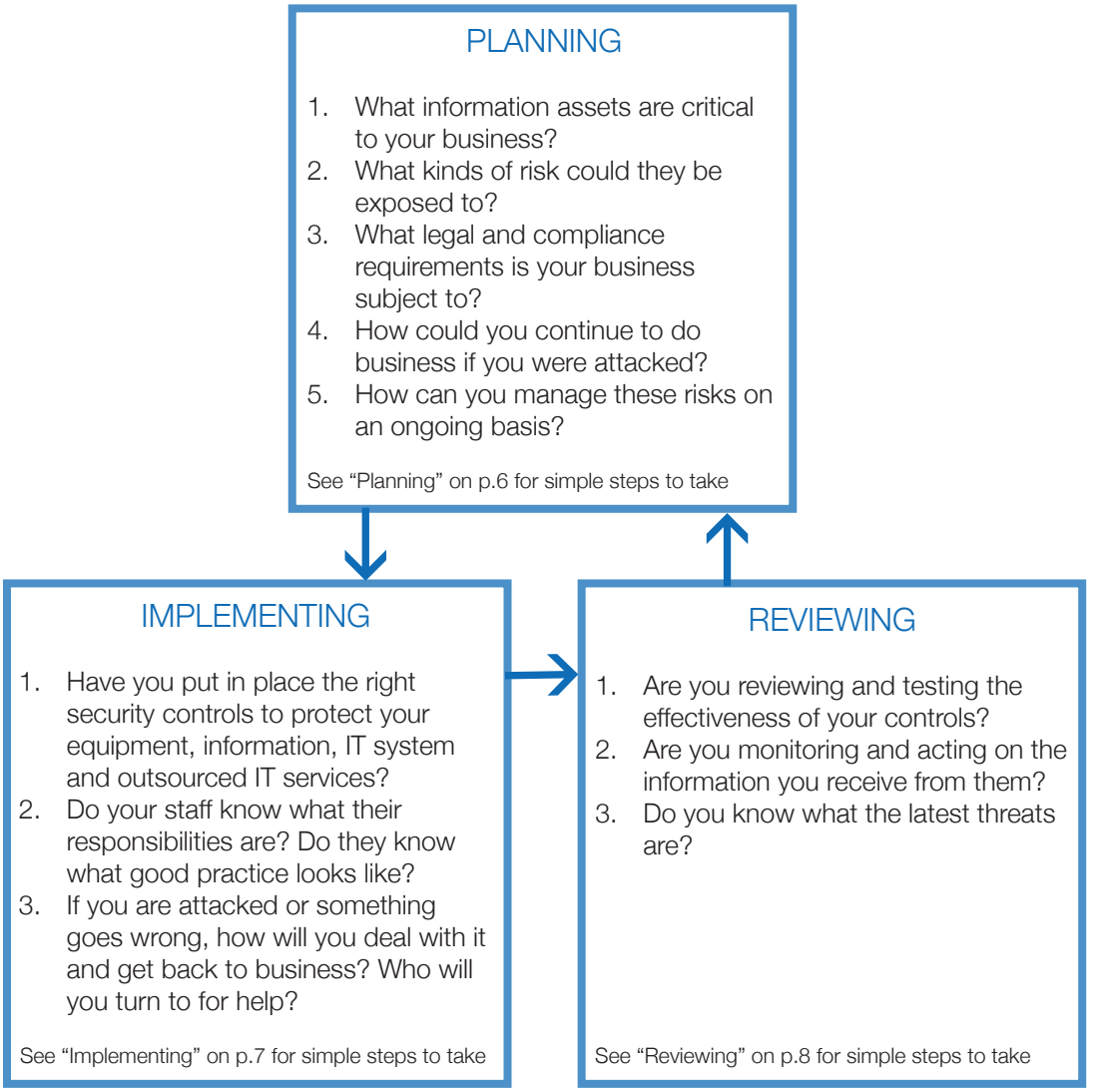
What impact could an attack have?

- Financial losses from theft of information, financial and bank details or money.
- Financial losses from disruption to trading and doing business – especially if you are dependent on doing business online.
- Costs from cleaning up affected systems and getting them up and running.
- Costs of fines if personal data is lost or compromised.
- Costs of losing business through damage to your reputation and customer base.
- Damage to other companies that you supply or are connected to.

How bad could it be?

A single successful attack could seriously damage your business.

How you can manage the risks



Planning

Take these steps to make information security part of your normal business risk management procedures.

- ❑ Consider whether your business could be a target - this will indicate the level of risk your business is exposed to. Ask around to see whether any of your suppliers, major customers or similar businesses in your area have been attacked, so you can learn from their experiences.

- ❑ Know whether you need to comply with personal data protection legislation and Payment Card Industry compliance (see p.10 for links to further information).

- ❑ Identify the financial and information assets that are critical to your business, and the IT services you rely on, such as the ability to take payments via your website. Assess all the IT equipment within your business, 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 your equipment and/or online services by your staff, third parties and customers, and whether it is enough to protect them.

- ❑ Ensure that your staff have appropriate awareness training, so that everyone understands their role in keeping the business secure.

- ❑ Decide whether you need to make an investment, or seek expert advice, to get the right security controls in place for your business. You could seek advice from accredited security consultants, internet and managed service providers or even your web designer if they have the capability.

- ❑ Consider who you could turn to for support if you are attacked, or if your online services are disrupted in some way. Define what your recovery procedures would be, and how you could keep your business running, particularly if you trade online.

Implementing

Take these steps to put the right security controls in place for your business. If you use third-party managed IT services, check your contracts and service level agreements, and ensure that whoever handles your systems and data has these security controls in place.

- Malware protection: install anti-virus solutions on all systems, and keep your software and web browsers up to date. Consider restricting access to inappropriate websites to lessen the risk of being exposed to malware. Create a policy governing when and how security updates should be installed.

- Network security: increase protection of your networks, including wireless networks, against external attacks through the use of firewalls, proxies, access lists and other measures.

- Secure configuration: maintain an inventory of all IT equipment and software. Identify a secure standard configuration for all existing and future IT equipment used by your business. Change any default passwords.

- Managing user privileges: restrict staff and third-party access to IT equipment, systems and information to the minimum required. Keep items physically secure to prevent unauthorised access.

- Home and mobile working, including use of personal devices for work: ensure that sensitive data is encrypted when stored or transmitted online so that data can only be accessed by authorised users.

- Removable media: restrict the use of removable media such as USB drives, CDs, DVDs and secure digital cards, and protect any data stored on such media to help stop data being lost and to prevent malware from being installed.

- Monitoring: monitor use of all equipment and IT systems, collect activity logs, and ensure that you have the capability to identify any unauthorised or malicious activity.

Reviewing

Take these steps to review your security and respond to any changes or problems you identify, including attacks or disruption to business.

- ❑ Test, monitor and improve your security controls on a regular basis to manage any change in the level of risk to your IT equipment, services and information.
- ❑ Remove any software or equipment that you no longer need, ensuring that no sensitive information is stored on it when disposed of. Review and manage any change in user access, such as the creation of accounts when staff arrive and deletion of accounts when they leave.
- ❑ If your business is disrupted or attacked, ensure that the response includes removing any ongoing threat such as malware, understanding the cause of the incident and, if appropriate, addressing any gaps in your security that have been identified following the incident.
- ❑ If you fall victim to online fraud or attack, you should report the incident to the police via the Action Fraud website. You may need to notify your customers and suppliers if their data has been compromised or lost (see p.10 for links to further information).

Scenario: small business loses important contract

What happened? A rival organisation with hostile intentions collected key information about a small manufacturing company over a period of time and used it against them. How? The attackers used social media sites to identify key employees and to get information about locations, contact details and current work projects. Armed with this information the adversary:

- sent targeted and realistic-seeming emails to a number of staff in different teams, containing attachments infected with malware;
- stole a work laptop from the managing director on a business trip.

The attacker used the malware capability together with the stolen laptop to get into the network and extract vital information about the company and its contract bid. They used this to produce a rival bid at a lower cost, using stolen intellectual property.

What was the impact? The company lost out on the contract. Without this work, it was impossible to maintain the full workforce and half of the employees were made redundant. This news was picked up by the local media, leading to lasting reputational damage and further loss of business.

What steps could have prevented this attack?

Planning

Risk management: considering what information assets the business held would have led to information about the contract bid being better protected.

Implementing

Staff awareness: training staff on the safe use of social media could have prevented so much sensitive company data being gathered from open sources.

Home and mobile working: An encrypted laptop with robust password protection could have prevented unauthorised user access to sensitive company data.

Where to get more information and advice

Get Safe Online

Practical advice on all aspects of cyber protection for small businesses at:
https://www.getsafeonline.org/businesses

Information Commissioner's Office (ICO)

Advice on your business' personal data responsibilities and obligations at:
http://ico.org.uk/for_organisations
Guidance on 1.) IT security with a focus on data protection issues, 2.) bring your own device (BYOD) and 3.) cloud computing at:
http://ico.org.uk/for_organisations/guidance_index/data_protection_and_privacy_and_electronic_communications

Payment Card Industry Security Standards Council

Advice on online trading and payment account data security at:
https://www.pcisecuritystandards.org/

Action Fraud

Report internet crime and find guidance on preventing fraud at:
http://www.actionfraud.police.uk/

HM Government

Cyber security guidance for businesses at:
https://www.gov.uk/government/publications/cyber-risk-management-a-board-level-responsibility
Information on the government's UK Cyber Security Strategy and programme at:
https://www.gov.uk/government/policies/keeping-the-uk-safe-in-cyberspace
Advice on technical measures at:
http://cpni.gov.uk/advice/cyber

Federation of Small Businesses (FSB)

Support and advice for members on a range of small business issues at:
http://www.fsb.org.uk

Intellect

Advice and support from the UK technology industry trade association at:
http://www.intellectuk.org/

This publication is available on our website at www.gov.uk/bis

Any enquiries regarding this publication should be sent to:
Department for Business, Innovation and Skills
1 Victoria Street
London SW1H 0ET
Tel: 020 7215 5000

If you require this publication in an alternative format, email enquiries@bis.gsi.gov.uk, or call 020 7215 5000.

URN BIS/13/780