HM Government

Small businesses:

What you need to know about cyber security

March 2015

BE CYBERSTREETWISE.COM

Contents page

What you need to know about cyber security

You've worked hard to build your business and make it a success. You're probably using a range of IT equipment and using the internet to advertise your business and sell online.

The internet brings huge business opportunities and benefits, but it also brings risks. Every day there are cyber attacks on UK companies like yours, attempting to steal your information and money, or disrupt your business. It is increasingly important to manage these risks to take advantage of the internet whilst protecting your business.

In 2014, 60% of small businesses experienced a cyber breach

The average cost of the worst breach was £65,000 - £115,000

You can keep your business safe and protect against online threats by putting some simple measures in place. This guide shows you how.

Make sure you get the basics right by always downloading software updates, using strong passwords and deleting suspicious emails. For more on how to get the basics right, see page 5.

By understanding the risks to your business and managing them effectively, you can help to ensure all aspects of your business are protected against online threats. For more on how to take a risk management approach, see page 6.

Cyber Essentials shows you how your business can protect against the common cyber threats seen online. Gaining the Cyber Essentials badge demonstrates your business takes this seriously.
For more on Cyber Essentials, see page 12.

CYBER ESSENTIALS

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, theft or destruction.

Good cyber security can enhance the reputation of your business and open up new commercial opportunities.

Most companies 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 financial transactions. The internet brings huge business 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 staff, 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. Simple measures can 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 – gaining the Cyber Essentials badge will help you do this. 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.

Getting the basics right

Taking some simple actions and practising safe behaviours will reduce the risk of online threats to your business.

Download software updates

Download software and app updates as soon as they appear. They contain vital security upgrades that keep your devices and business information safe.

Visit www.cyberstreetwise.com/software-updates for further advice on updates.

Use strong passwords

Use strong passwords made up of at least three random words. Using lower and upper case letters, numbers and symbols will make your passwords even stronger.

Visit www.cyberstreetwise.com/passwords for further advice on passwords.

Delete suspicious emails

Delete suspicious emails as they may contain fraudulent requests for information or links to viruses.

Visit www.cyberstreetwise.com/common-scams for further advice on suspicious emails.

Use anti-virus software

Your computers, tablets and smartphones can easily become infected by small pieces of software known as viruses or malware. Install internet security software like anti-virus on all your devices to help prevent infection.

Visit www.cyberstreetwise.com/security-software for further advice on security software.

Train your staff

Make your staff aware of cyber security threats and how to deal with them. The Government offers free online training courses tailored for you and your staff which take around 60 minutes to complete.

Visit www.nationalarchives.gov.uk/sme to find out more and take the course.

For further simple tips on how to protect your business, visit www.cyberstreetwise.com

Taking a risk management approach: Understanding the risks to your business

What is directly at risk?

Your money, your information, your reputation, your IT equipment and your IT-based services. 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 (i.e. 'in 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.

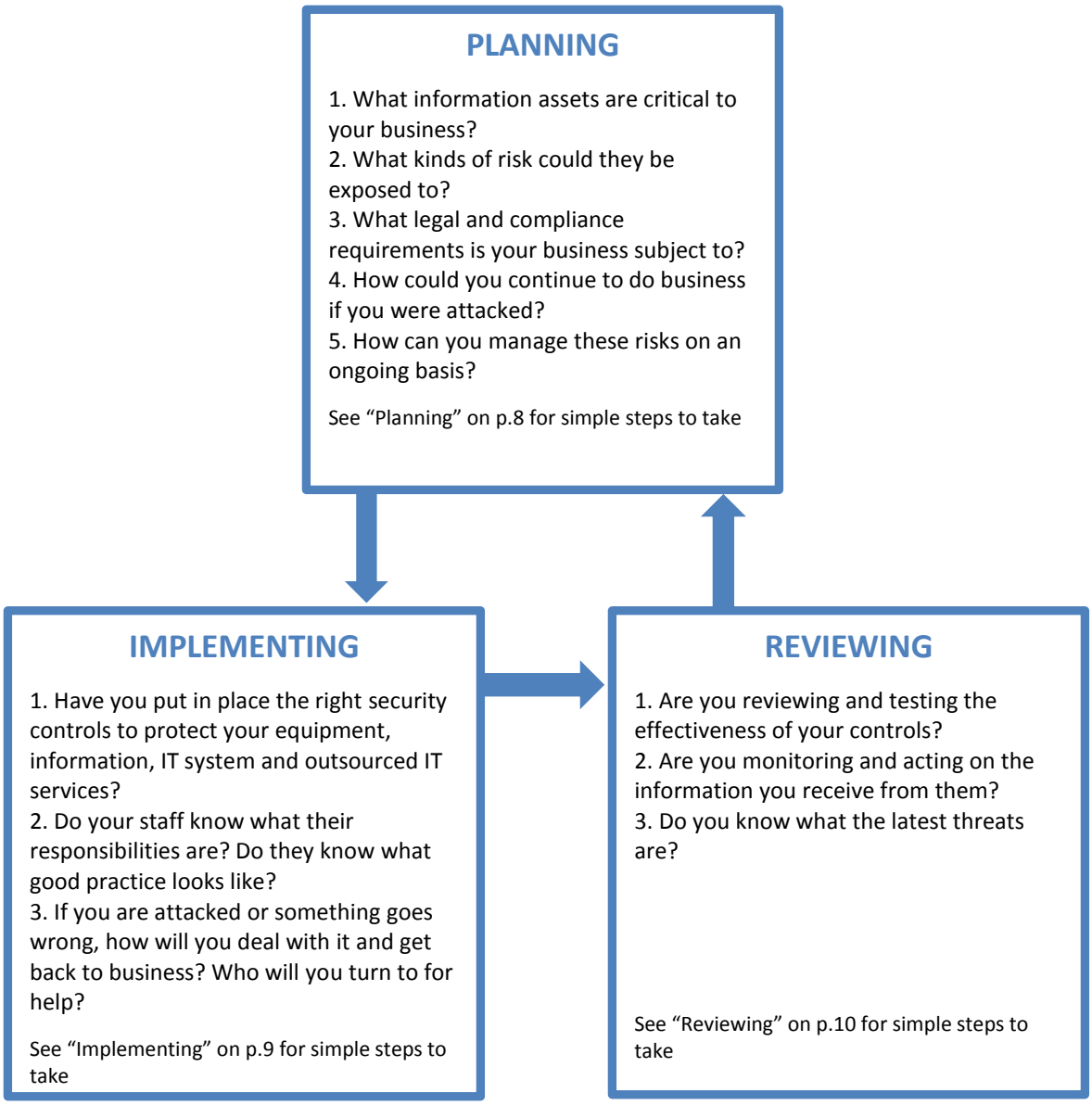
What impact could an attack have?

- Financial losses from theft of information, financial and bank details or money. The average cost of the worst security breach is between £65,000 and £115,000.
- Financial losses from disruption to trading and doing business – especially if you are dependent on doing business online. The worst breaches can result in a business being put of action for up to 10 days.
- Losing business from bad publicity & damage to your reputation & customer base.
- Costs from cleaning up affected systems and getting them up and running.
- Costs of fines if personal data is lost or compromised.
- 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.13 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.

- You may like to consider whether cyber insurance could protect your business against any impacts resulting from a cyber attack.

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 prevent data being lost and 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.13 for links to further information).

Scenario: small business loses important contract

What happened? A rival company 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.

Protect your business with Cyber Essentials

Once you've got the basics right and taken the steps outlined in this booklet, you are well on your way to becoming Cyber Essentials certified, which demonstrates to your customers you have good cyber security protections in place.

Cyber Essentials is a new Government-backed and industry supported scheme to help businesses protect themselves against the common cyber threats seen online. Government analysis shows the majority of online threats could be prevented if businesses put basic security measures in place. This booklet describes many of those measures. Cyber Essentials builds on this by clearly setting out the five key controls organisations should have in place to protect against common internet-based threats.

The Cyber Essentials documents are free to download and any organisation, large or small, can use the guidance to implement these essential security controls. Businesses can self-assess against the criteria, or seek independent verification and gain the Cyber Essentials badge, which enables your company to advertise the fact that it adheres to a Government endorsed standard. There are two levels of assurance to provide flexibility and affordability: Cyber Essentials and Cyber Essentials Plus.

Cyber Essentials is for all organisations, of all sizes, and in all sectors. This includes companies in the private sector, universities, charities, and public sector organisations. The Government encourages all organisations to adopt the requirements as appropriate to their business.

From October 2014, Cyber Essentials is mandatory for all suppliers of central Government contracts which involve handling personal information and providing certain ICT products and services. Many large firms are now adopting Cyber Essentials and will increasingly expect the businesses in their supply chains to hold Cyber Essentials certification too.

For more information and to use a quick, online self-assessment tool, visit:
www.cyberstreetwise.com/cyberessentials

Where to get more information, help and advice

Cyber Streetwise

The Cyber Streetwise campaign provides free, simple advice to help you and your business stay safe online.
www.cyberstreetwise.com

Free online training course

"Responsible for Information" is an information security training course for owners, managers and staff in small and medium sized businesses. It takes around 60 minutes and includes an introduction to protection against fraud and cyber crime.
www.nationalarchives.gov.uk/sme

Action Fraud

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

Business is GREAT campaign

'Do More Online' helps small businesses find customers and sell goods & services online:
www.greatbusiness.gov.uk/domoreonline

HM Government

£5,000 Innovation Vouchers are available which can be used by firms for advice to help protect and grow their business by having good cyber security.
https://vouchers.innovateuk.org/cyber-security

Information on the Government's UK Cyber Security Strategy and programme:
www.gov.uk/government/policies/keeping-the-uk-safe-in-cyberspace

Get Safe Online

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

Payment Card Industry Security Standards Council

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

Information Commissioner's Office (ICO)

Advice on your business' personal data responsibilities and obligations at:
https://ico.org.uk/for-organisations plus guidance on IT security and further advice and tools for small businesses.

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
cybersecurity@bis.gsi.gov.uk

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

URN BIS/15/147