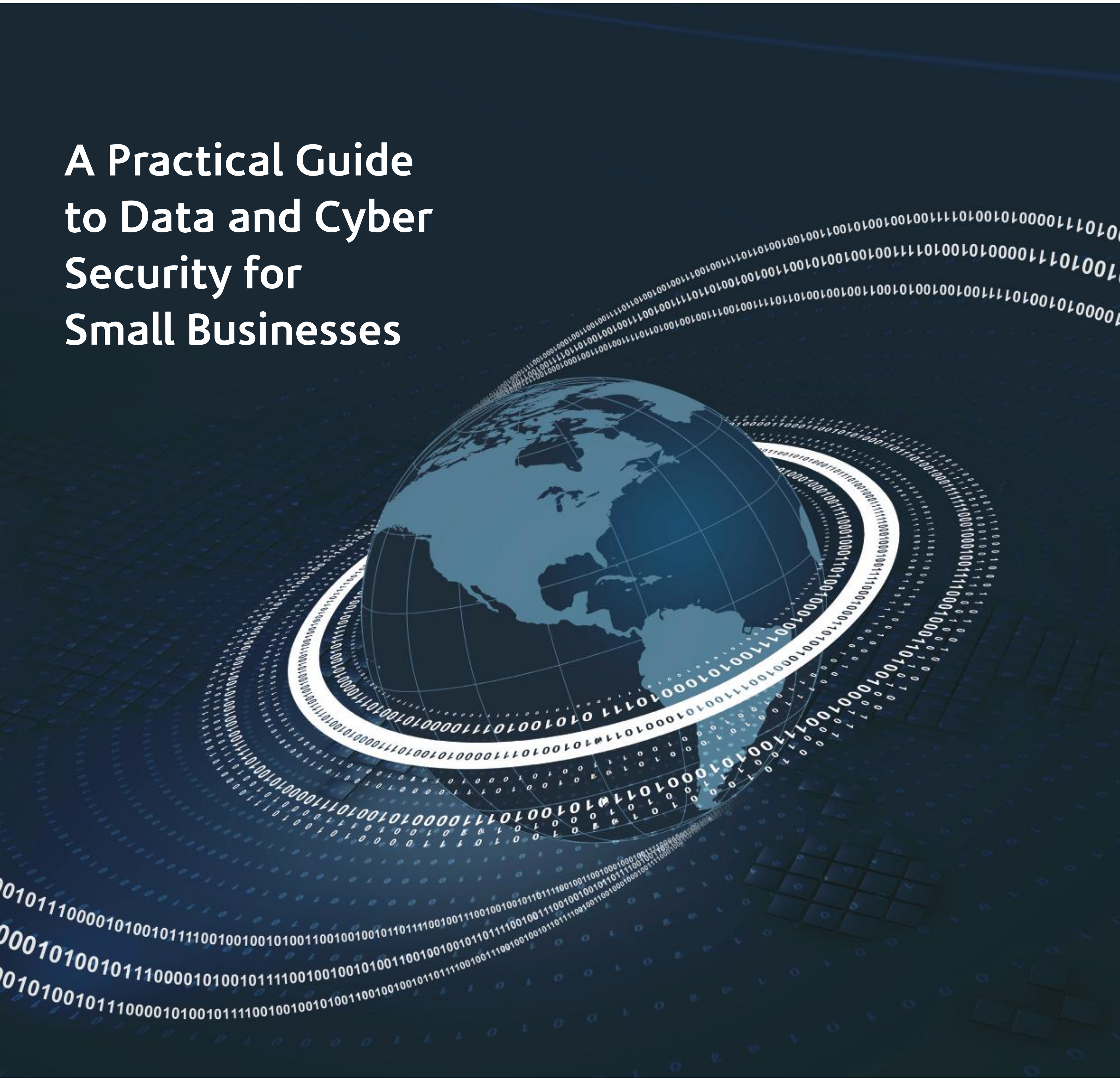
INTERNATIONAL INSTITUTE OF
RISK AND SAFETY MANAGEMENT

A Practical Guide to Data and Cyber Security for Small Businesses



Developed in partnership with ZURICH

Contents

> "As the threats from hackers across the globe increase there is no doubt that national and international laws will evolve"

1. Introduction

All organisations, big or small, make extensive use of electronic and non-electronic data in running their business and interacting with others in the modern and evolving commercial environment. While this can bring considerable improvement in effectiveness and efficiency in the way goods and services are delivered, it inevitably brings associated threats that can harm a small business and even endanger its survival. In the UK, the Data Protection Act states that "appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data". The Act therefore places the responsibility of protecting all types of data with the organisation itself, so data security should be considered at all times, including when assessing new business opportunities.

As the threats from hackers across the globe increase there is no doubt that national and international laws will evolve, and the onus on businesses to manage the risks and threats may become greater. As a result, businesses should take a proactive risk management approach to avoid facing costly reactive risk management measures later down the line.

Making sure your business's IT systems are safe and secure can be a complex task, and does require time, resource and sometimes specialist knowledge. If you have personal and commercially sensitive data within your IT system, you need to understand that it is likely to be at risk and take appropriate management and technical measures to secure it. The measures you put in place should be appropriate to the needs of your particular business, which may change as your business grows, and therefore needs to be kept under continual review.

The solutions to mitigate your risks need not be expensive, but must be effective. There are alternatives that could be considered depending on your circumstances and the maturity of your data management arrangements:

a) The ISO 27001 route gives you a standard to aspire to and if you wish permits associated third party certification to demonstrate the implementation of your data management system. This isn't the be all and end all but it does give you a framework to work to.

b) The free to download standard MSS 1000 has a section dedicated to managing data and has other sections covering the general management of business risks.

c) Another alternative is the UK Government developed Cyber Essentials Certification Scheme, which is a great start for smaller businesses and is designed to enable smaller businesses to better understand the risks they face and what needs to be done to mitigate and manage them.

"The solutions to mitigate your risks need not be expensive, but must be effective"

2. Why focus on data and cyber risk?

To begin with breaches of data protection legislation could lead to your business incurring a fine – up to £500,000 in serious cases. For many however, the reputational damage to your business could be much worse. Not only could you be negatively impacted by a loss of data or a system attack, but also by being unable to demonstrate that you have arrangements in place that meet best practice.

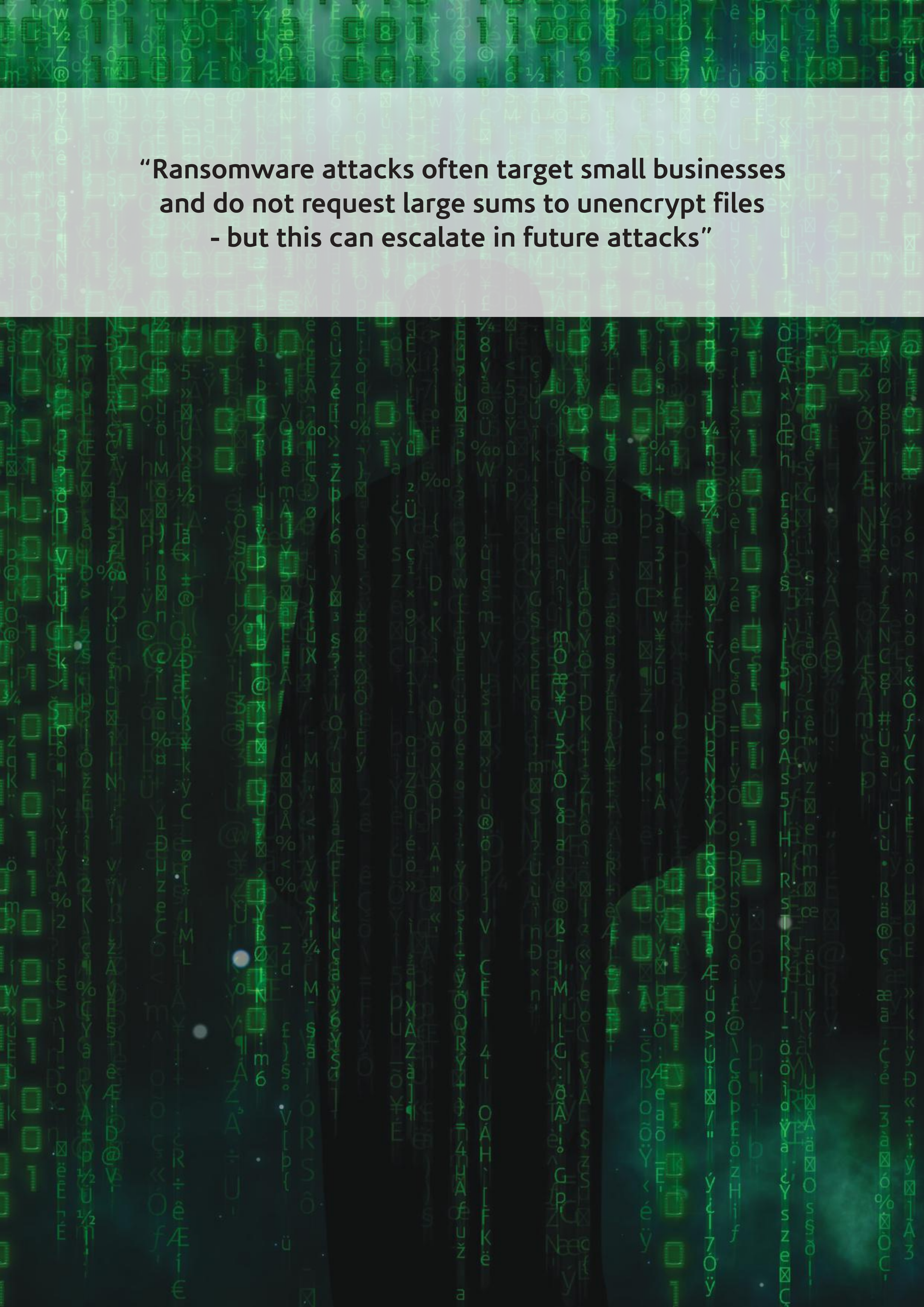
A data breach at Morrisons' Bradford head office last year cost the company more than £2m to rectify. More than 2,000 current and former staff are pursuing a group claim alleging that the retailer was ultimately responsible for breaches of privacy, confidence and data protection law.

A senior employee was jailed for eight years in July 2016 after he posted details of nearly 100,000 staff online. Information including salaries, national insurance numbers, dates of birth and bank account details were also sent to a number of newspapers. The employee leaked the data after being disciplined.

Whenever employers are given personal details of their staff, they have a duty to look after them. Most companies now gather and manage such material digitally and, as a result, it can be accessed and distributed relatively easily if the information is not protected.

Risk cannot be totally eliminated but it is critically important to be able to demonstrate that you have done everything reasonably practicable to reduce it to an acceptable level by following good practice.

The following are basic measures that you can put in place to prevent security breaches or limit the damage if they do occur.



“Ransomware attacks often target small businesses and do not request large sums to unencrypt files - but this can escalate in future attacks”

Step A: assess the risk to your business

Before you can establish what level of security is right for your business you will need to review the personal data you hold and assess the associated risks. You should consider all processes involved as you collect, store, use and dispose of personal data.

What personal data are we talking about?

This includes names and addresses… bank details… buying habits… opinions about an individual. For businesses, this is most likely to be customers, employees and those in their supply chain.

Under the Act, some personal information is deemed 'sensitive' and is therefore subject to greater restrictions. This includes information about someone's race or ethnicity, political affiliation/trade union membership, religious or moral beliefs, physical or mental health, sexuality and criminal record.

It is not just big businesses that are affected. Ransomware attacks often target small businesses and do not request large sums to unencrypt files - but this can escalate in future attacks. Malware – such as viruses and spyware - can result in a range of serious consequences for your business, including:

- Identity theft
- Fraud
- Invasion of personal privacy
- Theft, deletion and/or corruption of data
- Non-compliance with data protection rules
- A slow or unusable computer

Use an online assessment tool to determine the level of risk present in your business and assess your cyber security management processes.

Step B: document your policies and procedures to clearly state how you will manage data security and cyber risks

Defining your policies in written procedures provides clear direction and guidance to your staff and allows you to perform regular checks that they are being followed. It also provides a baseline for continual review to initiate improvement. It will also help facilitate third party certification if you decide to adopt it.

Step C: Consider how valuable, sensitive or confidential the information is and what damage or distress could be caused to individuals if there was a security breach

This enables your decisions and management controls to be risk informed and ensures that you are prioritising what is most critical and important to customers and other stakeholders such as investors and insurers etc.

Step D: With a clear view of the risks you can begin to choose the security measures that are appropriate for your needs

The aim is to create physical and/or administrative controls to reduce the identified risk to an acceptable level. You need to ensure that the likelihood and severity of any undesired event is minimised but also that contingency plans are effective if it does. Effective management of crisis critically depends on having well thought out arrangements tested and ready beforehand covering not only the technical matters but being able to communicate effectively and efficiently with customers and the media such that you appear to be professional and in full control of the situation.

Step E: Begin putting the measures in place

The risks will not reduce until you implement the risk control arrangements and your staff understand them and fully comply. You also need to continually monitor what you have implemented to ensure it is effective and remains so as things change.

3. Data security and cyber risk mitigation measures

There is no single solution that will provide a 100% guarantee of security for your business. The key to effective security is to have a layered approach, combining a number of different tools and techniques.

If one layer were to fail then others are in place to catch the threat.

3.1. Physical security

Equipment containing personal data could be stolen or damaged should an intruder break-in to business premises. You should ensure that personal and commercially sensitive data on your systems is protected against these threats.

Your computer servers should ideally be in a separate dedicated room with added protection. Back-up devices should not be left unattended and should be locked away when not in use and located so that they are unlikely to be impacted by the same damaging events e.g. fire, flood, adverse weather, burglary, malevolent action by an employee etc.

> “The key to effective security is to have a layered approach, combining a number of different tools and techniques”

3.2. Anti-malware protection

Malware is short for ‘malicious software’ and is any software used to disrupt computer operations, gather sensitive information, or gain access to private computer systems. It does not include software that causes unintentional harm due to some deficiency. Malware is an umbrella term used to refer to a variety of forms of hostile or intrusive software, including computer viruses, worms, trojan horses, ransomware, spyware, adware, scareware, and other malicious programs.

You should have anti-malware products regularly scanning your network to prevent or detect threats and make sure they are kept up-to-date. You should not allow any unauthorised software or data to be uploaded to your systems without the approval and control of competent persons.

3.3. Intrusion defence

You need to be able to prevent breaches happening before they penetrate deep into your network, for example, by using a well configured firewall and consider installing Intruder detection software to alert you to threats and attacks. The sooner you know you have an attack the quicker you can respond to the situation. Intrusion may originate from within your organisation as well as outside of it.

3.4. Access controls

Restrict access to your system to users and sources you trust. Each user must have their own username and password.

A ‘brute force password attack’ is a common method of attack, perhaps even by casual users trying to access your Wi-Fi, so you need to enforce strong passwords, limit the number of failed login attempts and enforce regular password changes. Consider two factor authentication or even biometric logins.

Passwords or other access should be cancelled immediately a staff member leaves the organisation or is absent for long periods.

3.5. Employee awareness and training

Employees at all levels need to be aware of their roles and responsibilities and made accountable.

Train your staff to recognise threats such as phishing emails and other malware, and how to take appropriate action, such as how to report suspicious emails.

3.6. Segmentation

You can prevent or limit the severity of data breaches by separating and limiting access between your network components. For example, your web server should be separate from your main file server. This means that if your website is compromised the attacker will not have direct access to your central data store.

3.7. Documented management system

A formal documented management system, including policies and procedures, will enable you to make sure you address the risks in a consistent manner and clearly communicate to your employees what is expected of them. Well-written documents should integrate well with your business processes.

Compliance with the management system and its effectiveness should be continually monitored, reviewed and if necessary amended to ensure that it remains fit for purpose.

3.8. Device hardening

Remove unused software and services from your devices. Older versions of some widespread software have well documented security vulnerabilities. If you don’t use it, then it is much easier to remove it than try to keep it up-to-date.

Make sure you have changed any default passwords used by software or hardware – these are well known by attackers.

3.9. Secure your data on the move

You need to ensure that an equivalent level of security is applied to personal data on devices being used away from the office as within it. Many data breaches arise from the theft or loss of a data device (eg. laptop, mobile phone or USB drive) but you should also consider the security surrounding data you might send by email or post.

You can take steps to reduce the effects of the theft by ensuring that personal data is either not on the device in the first place or that it has been appropriately secured so that it cannot be accessed.

ACTIONS

- Encryption is a means of ensuring that data can only be accessed by authorised users. Typically, a key (password) is required to 'unlock' the data.
    - Full disk encryption means that the all data on the computer is encrypted.
    - File encryption means that individual files are encrypted.
    - Your encryption key (password) should be a mix of upper and lowercase, numbers and special characters (i.e. #, &, !) and kept secret. Loss of the encryption key will prevent access to the data.
    - Some software offers password protection to stop people making changes to the data but this may not stop a thief reading the data. Make sure you know exactly what protection you are applying to your data.
- Some mobile devices support a remote disable or wipe facility. This allows you to send a signal to a lost or stolen device to locate it and, if necessary, securely delete all data.
    - Your devices will need to be pre-registered with a service like this.
    - Only transfer personal data to mobile devices if you actually need it and remove it when you have finished.

"Many people only find out they have been attacked when it is too late even though the warning signs were there"

3.10. Keep your systems up-to-date

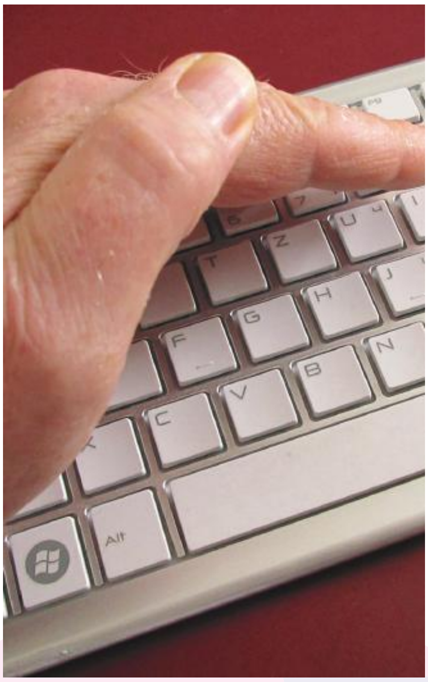
Computer equipment and software needs regular maintenance to keep it running smoothly and to fix any security vulnerabilities. Security software such as anti-malware needs regular updates in order to continue to provide adequate protection against evolving threats.

ACTIONS

- Make sure that security software is switched on and is monitoring all of your systems.
- Keep your software up-to-date by checking regularly for updates and applying them. Most software can be set to update automatically.
- Regularly review the protection you have in place on your system every two years to make sure that it is still adequate.
- You should also keep your knowledge of threats up-to-date by reading security bulletins or newsletters from organisations relevant to your business.
- You should also let your staff know about possible threats to your organisation. This could include alerting employees to the risks involved in posting information relating to your business activities on social networks or ensuring they know how to recognise phishing emails.

3.11. Keep an eye out for problems

Cyber criminals or malware can attack your systems and go unnoticed for a long time. Many people only find out they have been attacked when it is too late even though the warning signs were there.



ACTIONS

- Regularly check your security software messages, access control logs and other reporting systems you have in place.
- Make sure you can see what software or services are running on your network and are able to identify anything abnormal so that you take appropriate action.
- Run regular vulnerability scans and penetration tests to scan your systems for known vulnerabilities – make sure you address any vulnerabilities identified.

3.12. Do you know what you should be doing?

Some organisations do not have adequate levels of protection because they are not correctly using the security they already have, and are not always able to spot when there is a problem. You need to make sure that all your employees are aware of their roles and responsibilities and that they are clear about when action should be taken. You should also determine what actions should be taken if you suffer a data breach, cover them in your management system and test them before the event so that you know they will work.

ACTIONS

- Take the time to review what personal data you currently have and the means of protection you have in place.
- Make sure you are compliant with any industry guidance, legal requirements or contractual obligations.
- Document the controls you have in place and identify where you need to make improvements.
- Once any improvements are in place, continue to monitor the controls compliance and that they are effective, and make adjustments where necessary.
- Consider the risks for each type of personal and commercially sensitive data you hold and how you would manage a data breach. Creating a schedule of data types and requirements helps keep track of this.

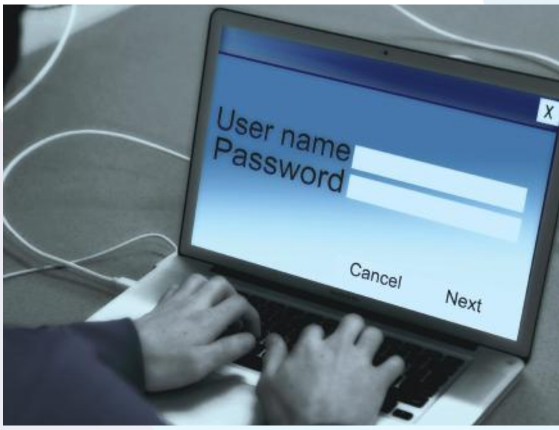
- Your management system should cover personnel competence and have training materials so that everyone knows their data protection responsibilities.
- Be prepared to get a security expert to review your systems - See this as an investment not a cost! – if you supply to a large organisation they may provide free assistance.
- Don't forget about backups of your data. Backups should be made regularly, kept secure in an appropriate location and properly deleted when no longer required.

3.13. Reduce the amount of personal data you hold

The UK Data Protection Act says that personal data should be accurate, up to date and kept for no longer than is necessary. Over time, you may have collected large amounts of personal data. Some of this data may be out-of-date and inaccurate or no longer useful.

ACTIONS

- Decide if you still need the data. If you do, is it stored in the right place?
- If you have data you need to keep but do not need to access regularly, move it to a more secure archive. This will help prevent unauthorised access.
- If the data is no longer needed, you should delete it otherwise you are incurring an unnecessary risk and possibly infringing legal or contractual requirements. This should be in line with your data retention and disposal policies as well as any contractual obligations you may have.
- You might need specialist software or assistance to do this securely and use certified destruction only.



3.14. Carefully monitor contractors, outsourcing and procurement

Many small businesses outsource some or all of their IT requirements to a third party. You also purchase hardware, software and other products and services that may affect your data security. You should be satisfied that they are treating your data with at least the same level of security as you would and that anything imported into your systems is of an appropriate quality and fit for your purpose.

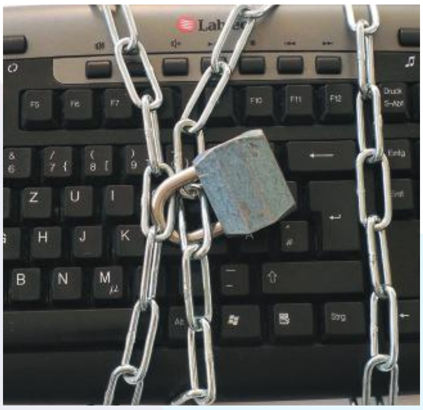
ACTIONS

- Ask for a security audit of the systems containing your data. This may help to identify any vulnerabilities which can then be addressed.
- Review copies of the security assessments of your IT providers.
- If appropriate, visit the premises of your IT provider to make sure they are as you would expect.
- Check the contracts you have in place. They must be in writing and must require your contractor to act only on your instructions and comply with certain obligations of the Data Protection Act.
- Don’t overlook asset disposal – if you use a contractor to erase data and dispose of or recycle your IT equipment, make sure they do it adequately. You may be held responsible if personal data gathered by you is extracted from your old IT equipment when it is resold.
- Maintain a list of approved critical suppliers with appropriate evidence demonstrating their competence and integrity.

4. More information

Further information is available to help you to assess the threat to your business, or to develop policies and protection, from the following:

- Managing Cyber Risk', APMG International whitepaper http://www.iirsm.org/cyber-security
- UK Government developed Cyber Essentials Certification Scheme.
- MSS 1000:2014 Management System Specification – Chartered Quality Institute.
- ISO/IEC 27001:2013 - Information technology - Security techniques - Information security management systems - Requirements.
- Information Commissioner's Office www.ico.org.uk/for-organisations
- Industry sector trade bodies.
- Relevant national professional bodies.
- National government agencies responsible for data security.



iirsm

INTERNATIONAL INSTITUTE OF
RISK AND SAFETY MANAGEMENT

International Institute of Risk & Safety Management
No 1 Farriers Yard, 77 Fulham Palace Rd, London W6 8JA
Tel: 020 8741 9100 Email: info@iirsm.org
www.iirsm.org