Acumenology

business support

UNDERSTANDING CYBER SECURITY FOR SMALL BUSINESSES

Understanding the risks of a security breach for your business

An Acumenology Business Guide
Acumenology.co.uk

Contents

01
Introduction

The internet brings huge opportunities and benefits, but with it also come risks.

Whilst traditionally larger companies have always been the target for cyber-attacks, most small business owners believe they are unlikely to affected as cyber-attacks are the concern of larger corporations.

However, recent trends have shown a considerable increase in smaller businesses also being targetedbecause hackers see them as 'soft targets' since they do not possess the same level of security as larger businesses.

With an increasing number of small businesses using their websites to store personal information about customers, employees and suppliers,combined with the introduction of new data privacy regulations (GDPR), it is essential that small businesses take relevant measures to review and strengthen their cybersecurity.

To further help you, Acumenology has produced a series of Business Guides on a range of relevant topics.
You can find these at: www.acumenology.co.uk/business-guides

This article was first published on December 2019 and may not necessarily match current events or current opinions and views of Acumenology Ltd. The information contained in this article is intended as a guide.

02

What is cyber security and how does it apply to my business?

Cyber security is the protection of information and digital assets from compromise, theft or loss.
The attack can be from an attacker outside, or an insider threat within your business.

Cyberattacks can occur in many different ways and are increasing in frequency.
As business increasingly rely on digital technology so cyber security must be made a priority.

Ask yourself the following questions.

Q. Have you looked at cyber security for your business?

Q. Do you have systems and processes in place to reduce the risk of a cyber-attack?

Q. Can your business withstand the disruption and potential financial loss from a cyber-attack?

03

What are the risks to your business?

What is at risk?

The risks are to the information you hold and to your IT systems and services.

The Information a business holds may include personal details on customers, employees and suppliers, credit card details if payment is being taken, your company's financial details together with sensitive information on pricing, product and so on.

Businesses are required to report to the Information Commissioners Office (ICO) any breach that results in personal information held being compromise.

This will inevitably lead to an investigation and review by the ICO of the security measures in place within your organisation.

There is also a risk to your IT services whether be they held on your own systems and devices or on third-party hosted systems.

Does your business have the resources needed to deal with any potential cyber-attack and it cope with the ensuing disruption?

Who could pose a threat?

The most likely source of threat is likely to be from:

- Current or former employees compromising your information either by accident, through negligence or, malicious intent.
- Criminals who wish to seek financial gain by causing you disruption

What form could the threat take?

Some of the most common forms of the threat are by:

- 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 employees.

What impact could it have on the business?

Make no bones, any cyber-attack is likely to have a significant impact on the business. This could be in the form of:

- 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 the affected systems and getting them running.
- Costs of fines if personal data is lost or compromised.

This article was first published on December 2019 and may not necessarily match current events or current opinions and views of Acumenology Ltd. The information contained in this article is intended as a guide.

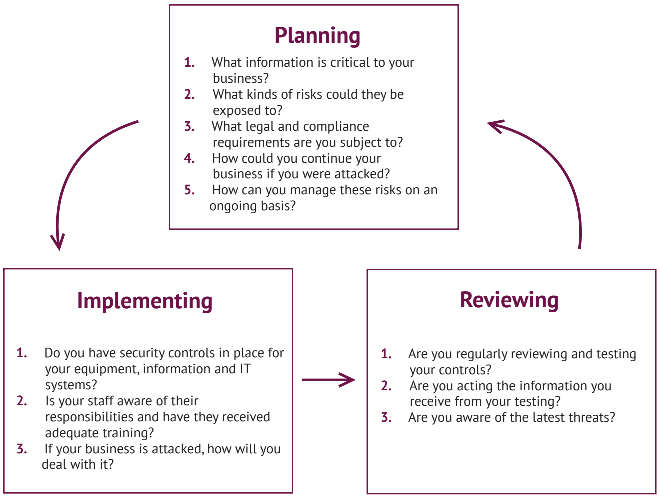
- Costs of losing business through damage to your reputation and customer base.
- Damage to other companies that you supply or are connected to.

A successful cyber-attack could seriously damage your business through significant disruption and financial loss.

04
How to reduce the risks.

Business owners and managers need to spend time in taking relevant action to mitigate the likelihood of a cyber-attack.

HM Government has developed a three-phase action plan as set out below.



Planning

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

Implementing

1. Do you have security controls in place for your equipment, information and IT systems?
2. Is your staff aware of their responsibilities and have they received adequate training?
3. If your business is attacked, how will you deal with it?

Reviewing

1. Are you regularly reviewing and testing your controls?
2. Are you acting the information you receive from your testing?
3. Are you aware of the latest threats?

05
Planning

Take the following steps to make information security part of your normal business risk management process.

- Consider whether your business could be a target - this will indicate the level of risk your business is exposed to.
- Know whether you need to comply with personal data protection legislation and Payment Card Industry compliance.
- 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 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 adequate.
- 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.
- Define what your recovery procedures would be, and how you could keep your business running, particularly if you trade online.

06
Implementing

The information provided in this section will help you put the right security controls in place for your business.

If you use third-party managed IT services, check your c and service level agreementsand ensure they too have adequate security controls in place.

This article was first published on December 2019 and may not necessarily match current events or current opinions and views of Acumenology Ltd. The information contained in this article is intended as a guide.

- **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 and ensure passwords are changed when staff leave.

- **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, 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.

- **Training**
  Ensure your employees are aware of their responsibilities and that they have received adequate training.
  The training should ideally be reinforced annually, and all new employees must also receive the training.
  Remember under GDPR regulations you are required to provide this training and provide evidence that you have done so.

07
Reviewing

Look at the activities set out in this section 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.

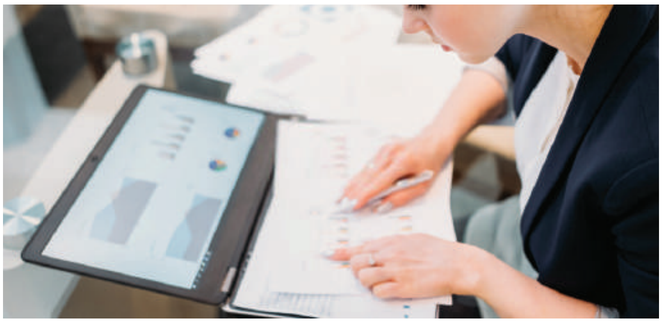
- Review and manage any change in user access, such as the creation of accounts when staff arrive and deletion of accounts when they leave.

- 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 as per the GDPR regulations.

  You will also need to notify the ICO.



This article was first published on December 2019 and may not necessarily match current events or current opinions and views of Acumenology Ltd. The information contained in this article is intended as a guide.

08

Further information

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.
http://ico.org.uk/for_organisations

Payment Card Industry Security Standards Council
Advice on online trading and payment account data security at: https://www.pcisecuritystandards.org/

The National Cyber Security Centre
Advice and guidance on a host of topics
https://www.ncsc.gov.uk/

09

Conclusion

With cyber-attacks getting increasingly frequent and an organisations responsibility under the new data privacy regulations – GDPR, businesses need to take a proactive approach in put in place relevant measures to strengthen their cyber security.
The potential financial consequences and disruption to the business can be so great that not doing so is taking a big risk

Acumenology has produced a series of Business Guides on a variety of topics relevant to starting and running a business.

These can be found at:
www.acumenology.co.uk/business-guides

This article was first published on December 2019 and may not necessarily match current events or current opinions and views of Acumenology Ltd. The information contained in this article is intended as a guide.