Think Ahead ACCA

Guide from

[insert your firm's name here]

Tel: [insert telephone number here] Email: [insert email address here] [Insert web address here]

[Insert a line about your business here]

IT security

Protecting your IT system and the information it holds is essential. An IT systems failure or data loss can be catastrophic for your business.

As well as installing security software, you need to look at physical security and the way you manage your IT systems. An effective backup routine is vital.

1. The threats

Computer viruses could infect your IT system

- Viruses are malicious computer programs created to damage IT systems.
- Some viruses are relatively harmless. For example, they may flash an annoying message on your screen.
- However, some are very dangerous. They can destroy data and disable your systems.

Spyware could become installed on your computers

- Spyware is software which runs on your computers without your knowledge.
- It typically sends details of your browsing habits (the websites you visit) to an online server.
- Some spyware is more dangerous and may record information you enter online. For instance, it may note your online banking login details, and send them to fraudsters who can then clean out your account.
- Spyware reduces your productivity by using valuable processing power.

You could be victim of a phishing scam

- Phishing scams involve fake emails and websites created by hackers posing as legitimate organisations.
- They try to dupe you into entering sensitive information into a website, like your name and bank details.
- This information can be used to steal your identity and/or your money.

Trojans could become installed on your system

- Trojans are harmful pieces of software which appear to be useful, but actually cause damage.
- Much like viruses, they can destroy data and cause serious harm to your business.

You could have problems dealing with spam

- Spam is junk email. It is also sometimes called 'unsolicited bulk email'.
- Receiving a large volume of spam can clog your email system.
- Spam messages often contain offensive or illegal content.
- Some spam promotes further scams; for instance, phishing emails are a kind of spam.
- Your system could be hijacked to send spam. This can cause your server to be blacklisted, so you cannot send or receive legitimate messages.

You should also consider physical security threats

- Criminals may steal your computer hardware.
- Fire, flood and other natural disasters could damage key hardware.

2. Security software

Install comprehensive security software on every computer in your business

- A security suite will include all the key protection you need.
- It is usually easier to buy a suite, but you can buy each piece of software separately. For example, you can buy separate virus and firewall packages.
- At a minimum, a computer security suite should include virus and Trojan protection, spyware protection and a firewall.
- Many packages also include spam filters, anti-phishing functions and more.
- Set up the software so it scans every computer regularly for threats.
- Security software should run automatically, and be set up so your employees cannot disable it.

Only use security software from reputable companies

- Well-established brands include McAfee and Symantec.

Make sure your firewalls are set up correctly

- A firewall blocks dubious internet traffic and stops hackers attacking your network.
- At minimum, install a software firewall on every computer in your business.
- Consider adding a hardware firewall too. This sits between your company network and the web, providing a first line of defence.
- If you have a server, a hardware firewall is essential.
- Firewalls should be set up to allow only essential network traffic through.

Keep all security software up to date

- New security threats are discovered daily.
- Security software companies regularly update their packages to protect against new risks.
- Set your security software to check for updates at least once a day.

3. Software control

Any software from outside your system can create a security risk

- The software itself may have security weaknesses or could create weaknesses in your system. For example, software which allows external access to your network.
- The software may be infected with a virus.

Control software installation

- Ensure only designated employees have the authority to install software and carry out regular software audits.
- Software downloaded from dubious sources is a major source of security problems.
- As a director you can be prosecuted and fined if your company uses pirated software.

Keep all your software up to date

- Software manufacturers release regular updates to fix bugs in their programs.
- Install updates as soon as possible once they are released. Most software, including Microsoft Windows and Microsoft Office, can do this automatically.
- Updates can occasionally conflict with other programs. If you have a large number of computers, test updates before rolling them out company-wide.

4. Access control

You reduce security threats by controlling access to your systems.

Give each employee their own username and password

- Your staff should be required to log in to use any part of your systems.
- Set up the network so that employees can only access the parts of the system they need. For example, only those in the HR department should be able to view employee records.

Establish password control procedures

- Use strong passwords. They should be longer than eight characters and use upper and lower case letters, numbers and symbols.
- Many operating systems (like Microsoft Windows) can be set up so employees are forced to choose strong passwords.
- Make sure passwords are kept secure. For instance, do not let employees write their passwords down.
- Do not let employees share log in details.
- Make sure employees lock computers or log off when they leave them unattended.
- Change passwords regularly. You may want to set them to expire every month so users are forced to change them.
- Change passwords when an employee leaves, or when a security breach is suspected. Promptly remove the accounts of former employees.

If you allow remote access, it is wise to add additional checks

- A virtual private network (VPN) is the most secure way to allow remote access to your network.
- For additional security, many VPNs require users to insert a smartcard in addition to entering a username and password.
- Setting up a VPN can be complicated. Your IT administrator or supplier can advise on security measures.

Control points of entry through which problem material could enter your system

- Make sure material entering your system is automatically checked for viruses.
- Consider disabling disk drives and USB ports to prevent employees copying files onto your system.
- Make sure wireless networks are using appropriate wireless security settings.

5. Backups

Without backups, any loss of your business data could be disastrous.

A backup system creates a safe copy of your important business data

- If anything goes wrong with your system, you can restore the data from the backup and continue working.
- Backups do not help prevent security problems, but they make recovery easier.

Your backup system should be robust

- You can backup onto removable media, like CD-ROMs, DVD-ROMs or tapes, or to another hard drive.
- Online backup services allow you to run backups across the internet. They can be very convenient, but ensure the backup company is trustworthy.

Put procedures in place to ensure your backups run correctly

- Set up a procedure for taking partial and complete backups.
- Make sure one staff member is responsible for ensuring the process works. Appoint a deputy to cover for their absence.
- Software is available to automate backups. Microsoft Windows includes a basic backup application.

Regularly test your backup procedures

- Many firms only discover their backup procedures have failed when trying to restore data after a disaster.
- You should test a full restore from your backup media every three months.
- Identify any weak points. For instance, does it take a long time to restore your data?
- Make contingency plans for disaster recovery. For example, what would you do if both your system and your backups became infected by a virus?

You may benefit from seeking help with your backup strategy

- Backups can save your business. If you lack in-house expertise, ask your IT supplier for assistance, or bring in a security consultant.

6. Physical security

You should take precautions to secure your hardware from theft and physical damage.

Isolate your most important hardware

- Make sure critical hardware is kept in a secure location. For instance, your server can be locked in a separate server room with restricted access.
- Make sure you control the environment your servers are kept in.

Be aware of the risks posed by unforeseen events and natural disasters

- Water destroys computer hardware. Keep all servers off the floor in case of flooding.
- Install a fire suppression system into your server room.
- Have a plan in place so you can relocate your main server(s) if necessary.

Keep individual computers secure

- Encourage your employees to follow good practice when out and about with IT equipment. For instance, issue employees with plain laptop bags or sleeves, rather than prominent branded bags.

Control how data is distributed in your business

- Do not allow employees to store sensitive data on their own computers. Instead, keep it on your server.
- Consider encrypting the hard drives of laptop PCs. This ensures thieves will be unable to access the data if they steal the machine.
- Avoid copying important data onto removable media like memory sticks. If you have to do this, ensure the data has been encrypted first.

7. Employees

The biggest risk for most businesses comes from their employees

Deliberately or accidentally, an employee may:

- fail to follow security procedures (for example, using another employee's password to save time);
- load harmful software onto computers;
- reveal confidential security information;
- bypass or disable security software.

Where appropriate, make security a recruitment issue

- The person who controls your passwords and security procedures is the greatest risk.
- Test attitudes to security in interviews and check the qualifications and references of IT employees carefully.

Make security a part of employees' contracts

- Clearly set out your security procedures and policies. Include computer security training in your induction sessions.

Contractors and temporary workers are a particular risk

- Issue them with their own passwords, and give them the absolute minimum of access to your system.
- Create accounts that expire automatically for temporary staff.

Security planning

Your security will not work unless you set up good procedures and follow them

- Make security a key element of your internet and email policies and distribute them to all employees.
- Taking immediate disciplinary action for security breaches can be counterproductive, encouraging employees to cover up future problems. Apportioning blame is less important than fixing the problem.
- Try to create a culture where everyone helps to identify potential security issues.

Assign clear responsibility for security

- Your network administrator will usually have responsibility for selecting and implementing security solutions.
- Top management must take overall responsibility. Directors can be held legally liable for the security of certain types of data.
- Taking security precautions could save your business, so bring in a consultant if you lack in-house expertise.

Signpost

- Find guidance on security software, staff policies, security planning and other aspects of IT security from Get Safe Online.

May 2018