ICAEW INFORMATION TECHNOLOGY FACULTY

2013
icaew.com/itfac

CHARTECH CYBER SECURITY

10 steps to cyber security for the smaller firm

ICAEW INFORMATION TECHNOLOGY FACULTY

THE TEAM

George Quigley
Chairman
T: +44 (0)20 7893 2522
E: George.quigley@bdo.co.uk

Jeremy Boss
Deputy chairman
T: 0300 068 5802
E: Jeremy.boss@DECC.gsi.gov.uk

Richard Anning
Head of IT Faculty
T: +44 (0)20 7920 8635
E: richard.anning@icaew.com

Paul Booth
Technical & development manager
T: +44 (0)20 7920 8476
E: paul.booth@icaew.com

Kirstin Gillon
Technical manager
T: +44 (0)20 7920 8538
E: kirstin.gillon@icaew.com

Tracy Gray
Services manager
T: +44 (0)20 7920 8526
E: tracy.gray@icaew.com

Contact details
IT Faculty
ICAEW
Chartered Accountants' Hall
Moorgate Place
London EC2R 6EA UK
☎ +44 (0)20 7920 8481
✉ itfac@icaew.com
icaew.com/itfac

Chartech is produced by
Progressive Customer Publishing
John Carpenter House
John Carpenter Street
London
EC4Y 0AN

Advertising enquiries to
advertising@progressivecp.com

To comment on your
magazine, please email us
at publishing@icaew.com

TECPLM12730

Printed in the UK by Sterling Solutions

10 steps to online security for SMEs

One of the most keenly debated subjects of the moment is cyber (or online) security – how businesses and individuals are at risk of having their data and identities compromised.

The government is doing a lot to make people aware, but many view this topic as something that either doesn't affect them or is not important enough to warrant their time or resource.

But today's business environment relies on digital technology to function; it brings great opportunity as well as risk. Business is undertaken more effectively and efficiently, but information flows can be intercepted and compromised. While online crime has often been viewed as an issue facing larger businesses, smaller organisations are increasingly coming into focus as the next soft target (with their intellectual property and customer and payment databases).

According to the latest 2013 Information Security Breaches survey, 87% of small businesses have reported a security breach this year (up from 76% a year ago). The average cost to a small business of its worst security breach of the year is estimated to be between £35,000 and £65,000.

However, by following a number of basic steps, organisations can significantly improve their online security and help safeguard their most important assets and trading relationships. Implementing a full Information Security Management System is best - but 'doing the basics' is a good place to start and can improve your chances of avoiding a compromise by up to 80%.

These 10 steps mirror and build on the *10 Steps to cyber security* issued by BIS (Department for Business, Innovation & Skills) aimed at larger organisations and available at https://www.gov.uk/government/publications/cyber-risk-management-a-board-level-responsibility.

Richard Anning
Head of faculty

10 STEPS TO ONLINE SECURITY FOR SMES

Following these basic steps will improve your chances of avoiding an online attack by as much as

80%*

1 Allocate responsibilities

2 Protect your computers and your network

3 Keep your computers up to date

4 Control employee access to computers and documents

5 Protect against viruses

6 Extend security beyond the office

7 Don't forget disks and drives

8 Plan for the worst

9 Educate your team

10 Keep records - and test your security

* As outlined by GCHQ in the *10 Steps to Cyber Security*

Username:

Administrator

Password:

●●●●●●●●●

1 ALLOCATE RESPONSIBILITIES

As with any business activity, in computer security it's crucial to identify what must be done and who will do it. Overall responsibility should rest with a senior manager who has a broad view of all the risks and how to tackle them. Other individuals can handle particular aspects - for instance, installing security software.

Management should identify the information and technology that's really vital to the business, where the big risks lie.

For example, damage to your financial system, or the loss of your customer list, could lead to the failure of the business. Other information may be less important.

Equally, some computers are probably more critical, or more vulnerable, then others. Identifying the risks, then establishing what security measures already exist and whether they work, and what extra ones are required, will help you to target your security efforts where they are most needed.

Buying security

While large organisations may need security consultants, smaller businesses can be well protected by security software bought online or at computer retailers. Usually, only basic knowledge is required to install it; built-in (default) settings will provide essential protection. More expertise might be needed for advanced features.

2 PROTECT YOUR COMPUTERS AND NETWORK

Malicious activity could come from outside or inside your business.

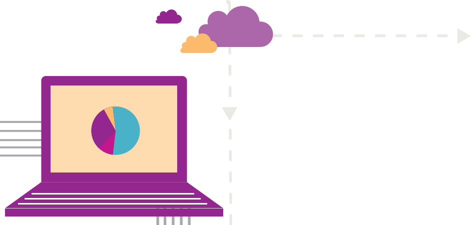
Attacks from outside, for example by troublemaking hackers or competitors, can be protected against by installing a firewall. This is software or hardware which examines all the computer communications flowing in and out of the business, and decides whether it's safe to let them through.

It can also be used to manage your staff's internet activity, for instance by blocking access to chat sites where employees might encounter security risks. You can set up (configure) the firewall to allow or prevent certain kinds of activity.

There are several different kinds of firewall. The router supplied by your Internet service provider (ISP) may already have one built-in, or you can buy a software firewall solution.

Protecting against illicit activity from inside the business requires other precautions we'll look at elswhere in this supplement. All of these also provide extra protection against attacks from outside.

REX FEATURES



3 KEEP YOUR COMPUTERS UP TO DATE

Suppliers of PCs, software, and operating systems such as Windows frequently issue software updates (patches) to fix minor problems (bugs) or improve security.

It's essential to keep all your computers up-to-date with the latest patches. Normally, they can be downloaded and installed automatically.

Remember that just one vulnerable computer puts all the others at risk. It's important to ensure that all available patches are applied to all of them.

4 CONTROL EMPLOYEE ACCESS TO COMPUTERS AND DOCUMENTS

Although your computers should be guarded by a firewall, you should still protect user accounts (each person's 'identity' with which they log on to a computer) and sensitive documents with passwords.

Because each individual should have a unique user name and a password, access to different parts of your IT can be limited to certain people. (Some individuals may have more than one user name and password, perhaps if they have multiple roles.)

This not only protects against accidental or intentional damage by staff to systems and information, it also provides further security against outside intrusions.

To achieve this, you can use security options built in to operating systems such as Windows, or you can buy specialised software online.
Because you identified your biggest security risks and most vital information in Step 1, you can decide whether password control for a given item should be basic (for instance, one password authorising access to an entire computer) or stronger (each document or application requiring a separate password).

Some individuals designated as computer administrators (admins) may be given access to nearly everything, in order to perform technical work. You should keep the number of admins to a minimum.

Security software will usually generate records showing which employees have used particular computers or documents at different times. This can be useful for pinpointing problems, but access to these records should, of course, be tightly limited - otherwise people misusing the system could alter them to cover their tracks.

Smart passwords

Passwords should be difficult to guess but memorable, and never written down. Some hackers employ 'dictionary attacks' which try every possible word until they find the right password. You can protect against this by ensuring that passwords include a combination of upper- and lower-case letters, numbers and symbols.

Require employees to change passwords regularly. Security software may be able to expire them after a set period, so that they have to be changed.

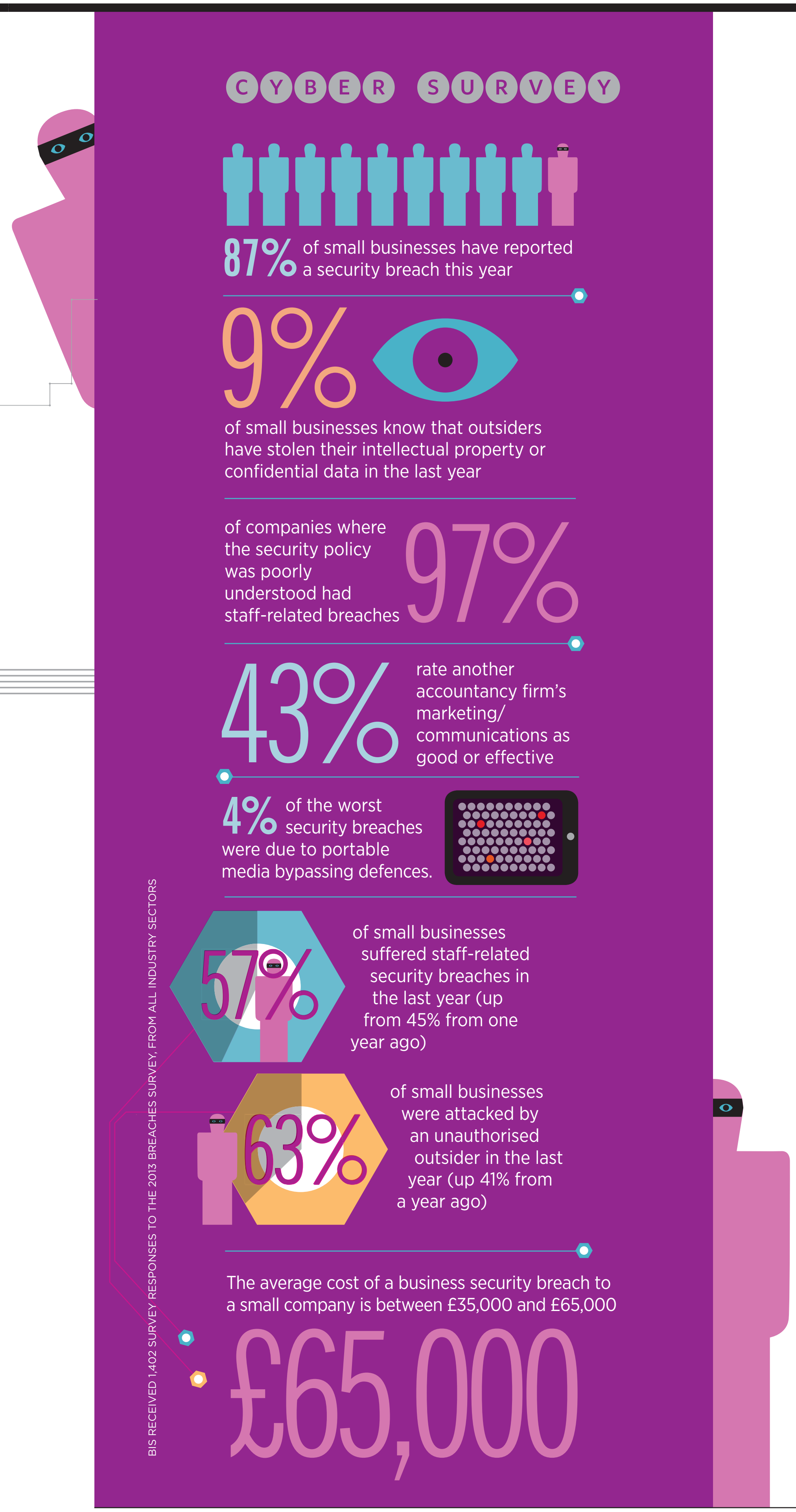
5 PROTECT AGAINST VIRUSES

Malicious software or 'malware' (a category including viruses, Trojans and spyware) may not always be as devastating as the headlines suggest, but can still slow down your systems dramatically, and passing them on to customers will win you no friends.

Fortunately, there is plenty of protection available. Your computers may have been sold with anti-virus software (the generic term, although most products also protect against other kinds of malware). If not, you can easily buy it.

This software regularly scans a computer in search of malware, deleting any that is found.

Regular updates to head off new threats are key to anti-virus software. So this is one area where it does pay to stick to the big brand names and to ensure that the software is set to receive updates as regularly as possible (ideally daily).



CYBER SURVEY

87% of small businesses have reported a security breach this year

9% of small businesses know that outsiders have stolen their intellectual property or confidential data in the last year

97% of companies where the security policy was poorly understood had staff-related breaches

43% rate another accountancy firm's marketing/communications as good or effective

4% of the worst security breaches were due to portable media bypassing defences.

57% of small businesses suffered staff-related security breaches in the last year (up from 45% from one year ago)

63% of small businesses were attacked by an unauthorised outsider in the last year (up 41% from a year ago)

The average cost of a business security breach to a small company is between £35,000 and £65,000

£65,000

BIS RECEIVED 1,402 SURVEY RESPONSES TO THE 2013 BREACHES SURVEY, FROM ALL INDUSTRY SECTORS

6 EXTEND SECURITY BEYOND THE OFFICE

Today's employees often work from home or on the road and use their own laptops, mobile phones, tablets and so on.

It is difficult to extend to these situations and devices the same level of security that you can apply to office computers. However, you can reduce risk by requiring that any personal equipment used for work is approved. At a minimum, it should have anti-virus software, password protection and, where applicable, a firewall.

To protect against unauthorised access to sensitive information when a phone or laptop is mislaid or stolen, it should be possible to delete all the information on it ('wipe' it) even when you don't physically have the device. This capability is built into some newer models; software can also be bought to perform remote wiping, but of course this must be installed before the device is lost.

Ensuring the sensitive data is kept in an encrypted area (see section 7) of the computer or device will stop most unauthorised attempts to access the data. This is very easy to set up using off-the-shelf software.

Safety in the cloud

More and more businesses are using cloud computing, where software is provided and documents are stored by a specialist company accessed via the internet, rather than on your own computers. This brings security considerations, though not necessarily extra risk.

You should ensure that your cloud computing provider takes security measures at least equal to those of your own business. They'll probably be better, but do ask detailed questions, and remember that if the provider is in another country, legal requirements may be different.

7 REMEMBER DISKS AND DRIVES

Removable disks and drives such as DVDs and USB sticks pose security risks in two ways. They can introduce malware into your computers, and they can be mislaid when containing sensitive information.

Ensure that as far as possible, only disks and drives owned by your business are used with your computers. Discourage employees from using them in third parties' computers (in Internet cafes for example), and set up anti-malware software to scan them whenever they are used in the office.

Establish a routine to track who has possession of each disk or drive at any given time, and check that all documents are erased from them after use.

Encryption

Extra-sensitive information can be encrypted for further security. Encryption transforms the contents of documents into apparently random sequences of characters, which can only be turned back into meaningful information when users enter a password (the key) or plug in a special device (a dongle).

Why does it matter to small practices?

"We don't hold banking details of our clients; our data is of no interest to a hacker." This is a sentiment I have come across a number of times in client meetings. My reaction is simple – to take a USB stick out of my pocket, hand it across the table to them and ask for a copy of all the data held in the organisation.

After an initial bemused reaction and a polite refusal to my request, I ask what data they have that they would not want to willingly hand over to me. This then starts the thought processes going. Perhaps they run a payroll and might be worried if salary details of clients got out of the building. Perhaps they file tax returns and accounts on behalf of their clients which need to be kept confidential. Perhaps they have other personal details of their clients they would not want divulged – or details of a financial transaction they are involved with. The list can actually be quite long.

If a small practice would be unwilling to hand over all their organisation's data to me on a USB stick, why would they run the risk of handing them over to competitors, troublemakers or irresponsible employees inadvertently through an online breach or a careless error? It is important to understand your critical data assets and take care to protect them, online as well as off. Following the simple steps in this guide will help reduce your risk and strengthen the service you can offer to your clients.

George Quigley, chairman IT Faculty and BDO partner

Why does it matter to me as a small business?

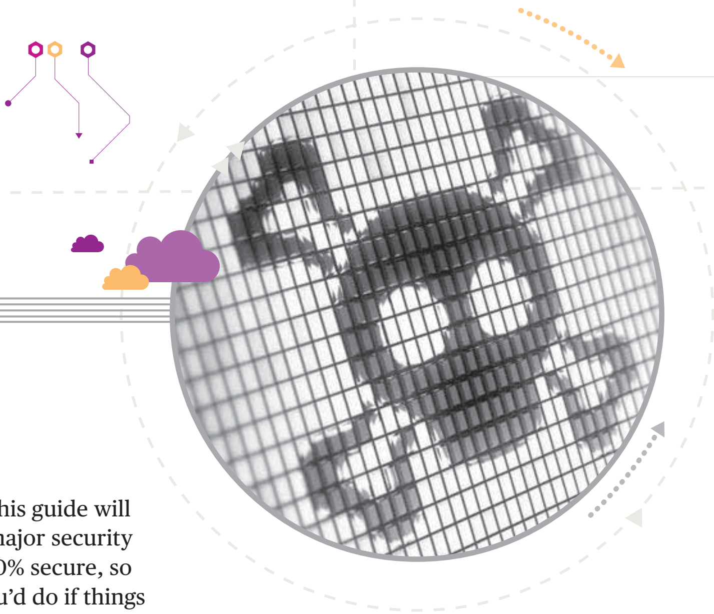
All the information within a company has a value, not just to that company but also to their competitors, organised crime, commercially or politically motivated hackers and others. You might be surprised what other people would find valuable, and no business is too small to be a target. If it's valuable to anyone, it's at risk. Of course, as soon as you start working with other organisations, you will also have a responsibility for protecting their data too.

Cyber incidents, including malicious or accidental data loss, can bring about huge financial burdens to a business, with direct financial loss estimated at £35,000-£65,000 for small businesses. Information Commissioner's Office (ICO) fines of up to £500,000 can also be levied if you breach the Data Protection Act.

No security can be 100% effective. People make mistakes, equipment fails and the threats keep changing. However, the threats are real for small and large business alike and are not going away. The simple steps outlined in this booklet will help protect against many of the common, low level cyber threats. If a company can apply these steps, it will help protect their own, their partners' and their customers' data.

Dr Emma Philpott, CEO The IASME Consortium

EYEVINE, REX FEATURES



8 PLAN FOR THE WORST

Following the measures in this guide will help you protect against a major security breach. But no system is 100% secure, so it's worth planning what you'd do if things went badly wrong.

First, define what is 'major' for you. Something that puts a non-critical department of the business offline for a couple of hours probably isn't. But something that prevents you serving customers, or performing vital functions such as payroll, will be.

Establish how you will know that there's a problem. You shouldn't have to wait for computers to go down; your firewall or anti-virus software, for example, may provide advance warning that something unusual is going on.

Plan your next steps. What help (perhaps a specialist computer company) should you call in? Do you need to contact key customers or suppliers to explain that there is a problem? Can some functions be continued using other computers, or pen and paper, while your systems are repaired?

Finally, ensure that it's clear who is responsible for doing what in an emergency. Your plan can be laid out in a document, and delivered in training sessions. It may incorporate elements of your plans for other disasters, such as a fire on your premises, and cut-down versions can be applied to less damaging computer incidents.

9 EDUCATE YOUR TEAM

Tell everyone in the business why security matters, and how they can help, using training sessions and written policy documents. This will encourage them to follow practices such as regular password changes.

Most will not have to actively work at security. They'll simply need to be aware of risks - for example, knowing that they should never click on a web link or attachment in an email from an unfamiliar source.

There are non-technical risks, too. One is social engineering, where hackers try to trick employees into revealing technical details that make your computers vulnerable. For example, a hacker might pretend to work for your computer supplier and claim they need passwords to perform maintenance.

The casual atmosphere of social media such as Facebook could be conducive to such deceptions, so employees should be especially wary of discussing your systems and practices on social media.

Don't panic

Security matters, but it is also important that team members do not become so paralysed by fear that they – and your business – lose out on the many benefits of the online world, or even reject contact with potential customers. Sensible caution is often better than absolute bans.

10 KEEP RECORDS AND TEST YOUR SECURITY

Security is an ongoing process, not a one-off fix. So it's important to keep clear records.

For example, the decision making in Step 1 of this guide could help you produce a list of all your hardware and software, along with an indication of how secure each item needs to be.

Similarly, records of software patches and lists of authorised personal devices will help build up a picture of your business's security status, spot potential weak points, and figure out how any problems arose.

Good record keeping will also help you regularly test all your security measures, and ensure that you have functioning, up-to-date software. Any business is only as secure as its weakest link, and testing will make sure that no weaknesses are overlooked.

Useful links

The faculty resource centre
icaew.com/cyber

Cyber security: what small businesses need to know – advice from BIS **gov.uk/government/publications/cyber-security-what-small-businesses-need-to-know**

Information Commissioners Office
ico.org.uk

Get Safe Online
Getsafeonline.org/businesses

MAKING IT WORK FOR YOU

If you are an accountant in practice or in business, we can keep you up to date with IT issues and developments. We will represent your interests and expertise and help you make the best possible use of IT.

MEMBER BENEFITS

- One stop shop: all the resources you need in one place.
- Publications: technical information in a simple easily digested format.
- Excel Community: regular updates from Excel experts and full access to a suite of online training.
- Online community: IT Counts lets you share up-to-the-minute IT news and views.
- Research: projects including surveys to improve insight into accountants’ use of IT.
- Events: both online and live, London and regional, with discounted rates for members.
- Thought leadership: working in the public interest to improve IT in the profession.
- Career development: full support, with resources to chart your development.

All accountants are affected by IT and need to understand the implications for their businesses, their practices and their clients. The IT Faculty is here to help you get the most from the IT you already have, and offer advice about what, where and when you may want to upgrade or expand.

linkedin.com – find ICAEW

twitter.com/icaew_ITFaculty

ICAEW

INFORMATION
TECHNOLOGY
FACULTY

BUSINESS WITH CONFIDENCE

icaew.com/itfac