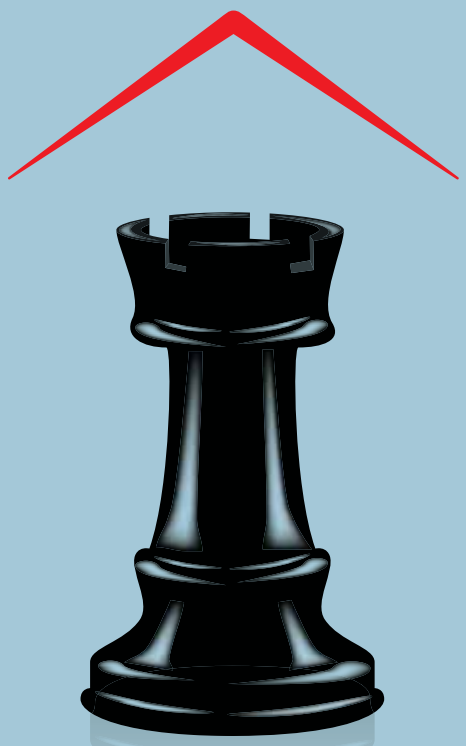
TECH ESSENTIALS
IT FACULTY



10 steps to cyber security for smaller firms

Keeping up to date to stay ahead

This is the third edition of our *10 Steps to Cyber Security* guide and it is increasingly clear with every issue that we can't get these simple messages out often enough. While the fundamentals on how to protect yourself, your business and your clients remain essentially unchanged, the context in which we write about them continues to shift. Cyber criminals are always finding new means of attack and we all need to keep up to keep them out.

As a result, cyber security remains one of the most important areas for our faculty. This is no surprise, given the universal and ever-shifting nature of the threat. We continue to work closely with government, as well as those from all sectors and all parts of the profession as well as the wider business community. It matters because regardless of whether you're a FTSE 100 board director, run a small business, work in practice or the public sector, this is a subject you can't afford to ignore or get wrong.

Since we published the last version of *10 Steps to Cyber Security* we have continued to work to help organisations of all sizes put this issue at the heart of their leadership agendas. Recent attacks highlight the apparent ease with which even large, established and well prepared organisations unwittingly invite hackers in, and the damage they suffer as a result.

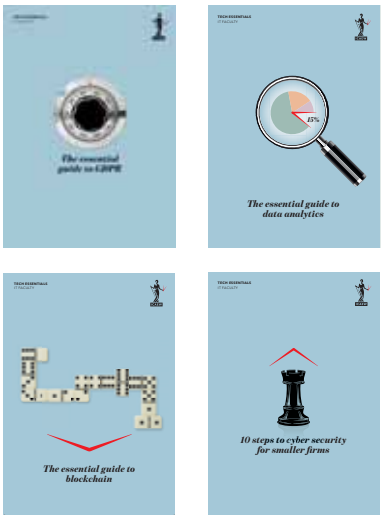
Having worked with the UK government on the creation of its Cyber Essentials scheme, we continue to support it. It sets a level of basic cyber hygiene and reduces the chances of a cyber attack by as much as 80%.

In a world that is continually shifting, it is a surprise to find anything constant. But over the last few years, our series of *Audit Insights: Cyber Security* reports, based on the findings of the top six audit firms and their interactions with clients, have continued to raise the same four flags. It still shocks me that organisations of all sizes (particularly the largest ones) are still not 'doing the basics', making it easier for criminals to get in. For information, visit icaew.com/auditinsights

We continue to track new legislation, noting directives such as GDPR and other regulation that affects you. Advice on this and all of our output is available online at our cyber security resource centre at icaew.com/cyber

We welcome your feedback, as well as any questions or suggestions you have on what else we can do to help you.

RICHARD ANNING
Head of IT Faculty, ICAEW



THE TECH ESSENTIALS SERIES
This latest cyber security briefing is the fourth guide in our Tech Essentials series. Tech Essentials guides are designed to update members on the latest technology issues affecting and transforming the accountancy profession. Previous guides have covered GDPR, data analytics and blockchain. We will continue to bring you practical tips and expert insight over the coming months. To obtain copies of past guides that you have missed, visit icaew.com/techessentials or email itfac@icaew.com

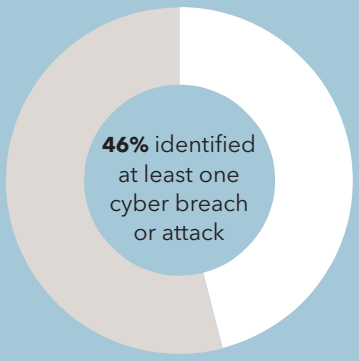
Our dedicated IT security hub is at icaew.com/cyber

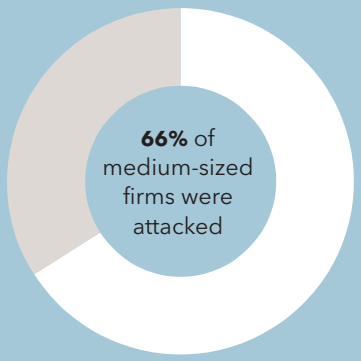
CYBER SECURITY FACTS AND FIGURES

£29,100,000,000

Cost of cyber crime to 2.9m British businesses in 2016

Of all UK businesses in the past year:





The most common types of breach in the past 12 months:

27% People impersonating the organisation in email or online

17% Ransomware

72% Fraudulent emails

33% Viruses, spyware and malware

20% of businesses had put staff through cyber security training in the past 12 months

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

ALL STATISTICS: BEAMING; CYBER SECURITY BREACHES SURVEY 2017

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 than others. Identifying the risks, establishing what security measures already exist and whether they work – and finding out what extra ones are required – will help you to target your security efforts where they are most needed.

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 that 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 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, but we'll look at those elsewhere in this supplement (see step 4 and the box *Practical pointers: some advice from ICAEW*, page 8).

'Cyber incidents, including both malicious and accidental data loss, can create huge financial burdens for a business. The financial losses may not just be from potential fines but also from the consequential reputational damage'

DR EMMA PHILPOTT
CEO, the IASME Consortium

ONE MAN'S TRASH IS ANOTHER MAN'S TREASURE

Dr Emma Philpott, CEO of the IASME Consortium, explains how the most inconsequential information can have huge value in the wrong hands

All information within a company has a value, and not just to that company. Other interested parties can include competitors, organised criminals, commercially or politically motivated hackers, disgruntled employees and many others. You might be surprised what other people find valuable, and no business is too small to be a target. If information has a value to any one party, then it's a risk to your business.

Companies need to consider what the consequences of an accidental loss of data as a result of human error would be. Of course, as soon as you work with other organisations, you will also have a responsibility for protecting their data too.

Cyber incidents, including both malicious and accidental data loss, can create huge financial burdens for a business. The financial losses may not just be from potential fines but also from the consequential reputational damage.

From May 2018 the new General Data Protection Regulation (GDPR) will make it mandatory to report certain data breaches (see box, *Cyber and the GDPR*, page 10). Organisations may be fined large amounts for not protecting personal information adequately, whether a data breach has taken place or not.

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 businesses alike and are not going away. The simple steps outlined in this booklet will help protect against many of the common cyber threats. If a company can apply these steps, it will help protect its own, its partners' and its customers' data.

To this end, the IASME Consortium created the IASME Governance Standard in 2013. Although suitable for organisations of all sizes and across all sectors, the IASME Governance Standard offers SME businesses an Information Assurance certification option that is more practical to achieve and maintain than ISO 270001.

The standard is risk based and includes aspects such as physical security, staff awareness and data backup. The IASME governance assessment now also includes the option of a review against the GDPR requirements.

The IASME Consortium is a leading Accreditation Body appointed by the government to deliver Cyber Essentials via trained and licensed certification bodies.

You can learn about approaches to certification, including companies that are licensed to deliver IASME assessments, and routes to becoming an assessor on the website included in the resources section on page 11.

3

Keep your computers and devices 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 and devices up to date with the latest patches. They can usually be downloaded and installed automatically. Remember that just one vulnerable computer puts all the others at risk – so it's important to ensure that all available patches are applied to all machines.

RANSOMWARE

The most famous recent example of ransomware, WannaCry, hit the NHS in May. Files at multiple trusts were encrypted by hackers who then demanded between $300-$600 to release them. The NHS was not alone in being targeted this year; computers in 150 countries have been affected. Such ransomware is an apparently growing phenomenon: in the case of WannaCry, hackers exploited a vulnerability caused by PC users failing to upgrade from the obsolete package Windows XP. There is still some debate about whether those affected were sent infected emails or if the virus infiltrated systems directly by exploiting the vulnerability in out-of-date systems. Microsoft issued a patch against WannaCry in March; but success against ransomware depends on people realising that they need to shore up their computers.

Having weak passwords, it has been suggested, also helps hackers gain access when businesses don't use the latest software and update it regularly.

As well as following industry guidance on such upgrades, businesses need to remain alert to what is going on in the wider world when it comes to hacking attempts and the latest malware or scams – this will help managers decide whether current processes remain strong enough. Dealing with the likelihood of a cyber breach is not a one-off exercise, but a live, ongoing management issue.

68

Mean number of breaches in a year suffered by businesses of all sizes

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/passphrases.

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 (though 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.

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).

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. Gartner predicts the worldwide public cloud services market will have grown 18% in 2017. Cloud 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.

CYBER ESSENTIALS: WHERE IT ALL BEGAN

Launched in 2014 at Chartered Accountants' Hall, the Cyber Essentials (CE) scheme was envisaged as a key objective of the National Cyber Security Strategy, and was delivered as part of the government's National Cyber Security Programme.

Since October 2014, the UK government has required all suppliers bidding for certain personal and sensitive information handling contracts to be CE certified.

CE is still being championed in the government's *National Cyber Security Strategy 2016-2021*. Proper implementation of CE, it argues, 'will protect against the vast majority of common internet threats'.

The CE scheme focuses on the most common internet-based cyber security threats, and reviews the five technical controls – access control; boundary firewalls and internet gateways; malware protection; patch management and secure configuration – that organisations should focus on.

Its requirements reflect longer-established and more extensive IT security standards, such as the ISO/IEC 27000 series. There is no law to say a business must be ISO 27000 series compliant, and many may find that CE is more than adequate for their needs and reputation.

Paul Rolison, director, Cyber Strategies, explains the thinking behind Cyber Essentials (see left) while below he discusses life as a Cyber Essentials assessor

CYBER ESSENTIALS: THE NITTY GRITTY

I am a chartered accountant who has been working in the world of IT since qualifying in the early 1980s. My journey has led me down a curious path to my principal role as a CE assessor. The role combines the principles of auditing (which are engrained) with the technical background of IT infrastructure and networking generally.

Since 2014 when the government launched CE, the take up by businesses and organisations has moved slowly along its own exponential curve. The pace of take up during 2017 has increased significantly and this has been driven by: requirements within primarily central government contracts and more recently by wider government contracts; supply chain requirements from security-aware and focused entities; and greater awareness by businesses that they need to do something to safeguard their data and, in turn, their business.

I spend the majority of my time either undertaking or managing the independent assessments of businesses that wish to achieve the higher level of CE Plus. This does not require any further work on the part of the business beyond submitting their answers to the CE online portal. The independent assessment is carried out based upon a government test specification.

So how does CE help? The standard essentially requires IT infrastructure to be securely configured – there is rarely a need to invest in further systems to achieve the standard unless unsupported software remains in use, such as Windows XP. The problems I find on almost every site visit include: software still installed that is not required, which in turn usually means it has not been updated (for example, Adobe products, pdf readers, zip apps); user accounts still active for staff who have left; and most importantly, security patches not up to date.

The key message is that many businesses think their systems are secure, but when tested many holes are found. Once the remediation work has been completed, there is little doubt in my mind that the business is not only far more secure but has also learned a great deal more about security along the way.

6

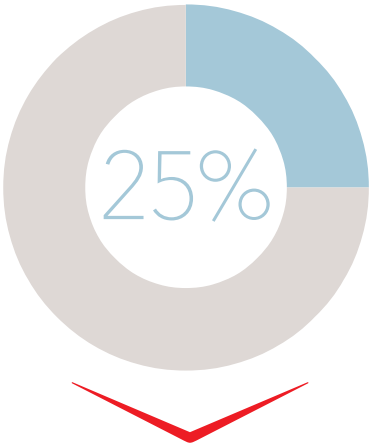
Extend security beyond the office

Today's employees often work from home or on the road using their own laptops, phones and tablets. It is difficult to extend the same level of security you can apply to office computers to these devices. But you can reduce risk by requiring approval of any personal equipment used for work. It should have the minimum of anti-virus software, password protection and (where applicable) a firewall. And to protect against unauthorised access to information when a device is mislaid or stolen, it should be possible to delete all the information (wipe it) even when you don't have the device. This capability is built into newer models; software can also be bought to perform remote wiping, but this must be installed before the device is lost. Ensuring the sensitive data is kept in an encrypted area (see step 7) of the computer or device will stop most attempts to access data. This is easy to set up using off-the-shelf software. Beware of the dangers when connecting to unencrypted public wifi, as hackers can intercept data. Check the hotspot is genuine and make sure file sharing is off and the firewall is on.

7

Remember to secure disks and drives

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



1/4 of businesses reported their breach to anyone other than a security provider

'You'll thank yourself if you address the 'what if it happened to me?' scenario. Plan ahead and don't keep all your eggs in one IT basket. Regular back-ups (kept off-site) and up-to-date contact lists of who you'll want to call if hackers breach your defences will minimise disruption and cost'

PAUL SIMKINS
Director of quality assurance, professional standards, ICAEW

PRACTICAL POINTERS: SOME ADVICE FROM ICAEW

No one is exempt from a cyber attack. With an increase in gaming mentality, these days it's as much about racking up spectacular numbers of victims and creating maximum disruption as it is about extracting money.

This is no time to be a rabbit in the headlights – better protection and better damage limitation can reduce the risk of attack and minimise its cost as hackers get smarter and bolder by the month.

Increasingly we hear that simple, protective measures can dramatically improve your odds. Adopting unpredictable and more complex passwords/encryption is just one good example – and there are now websites where you can check how long it would take to hack your personal favourites (see page 11). Providing regular awareness updates for all staff can also prevent some of the cheekier online social engineering methods from breaching established controls.

And, should the worst happen, you'll thank yourself if you address the 'what if it happened to me?' scenario. Plan ahead and don't keep all your eggs in one IT basket. Regular back-ups (kept off-site) and up-to-date contact lists of who you'll want to call if hackers breach your defences will minimise disruption and cost. Naturally, your trusted IT specialists (who should also have a plan), key staff members, key clients and stakeholders should be on your list – but also should those who can help if the attack occurs outside of business hours (hackers don't always attack during nine-to-five). Don't forget to print these lists and keep them off-site and out of sight.

Finally, the physical security of your premises can often be overlooked. Intruders can borrow invaluable reminders of the latest password stuck to a display screen or the inside of a drawer – or find clues left on a desk to poorly considered passcodes or business secrets – so think fortress!

Don't underestimate hackers – they're smart, sneaky, competitive and ruthless.

Paul Simkins, director of quality assurance, professional standards, ICAEW

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 should you call in? A specialist computer company perhaps? 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.

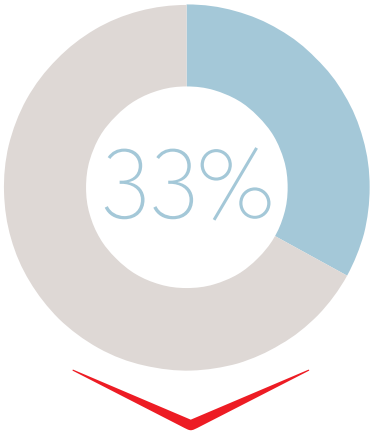
Most will not have to actively work at security, they'll simply need to be aware of risks – for example, knowing that they should never click on a web link or attachment in an email from an unfamiliar source.

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

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. Keeping good records 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.



1/3 of businesses had a formal cyber security risk policy in 2016

The new regulation does not specify how an entity must protect its systems, but it does outline the expected level of care to be taken – and a €20m or 4% fine for non-compliance is the incentive to act

CYBER AND THE GDPR

By 25 May 2018, all UK organisations handling personal and sensitive data as part of their business operations will need to be compliant with the General Data Protection Regulation, which supersedes the Data Protection Act 1998. This will be implemented before Brexit, after which time a new piece of UK legislation is expected to be brought in, largely mirroring aspects of GDPR.

The new regulation does not specify how an entity must protect its systems, but it does outline the expected level of care to be taken – and a €20m or 4% fine for non-compliance is the incentive to act. One key change less often repeated is the shared responsibility for compliance by both data processors and data controllers, as opposed to just controllers under the old rules. Not implementing data protection by design, using data protection impact assessments or maintaining appropriate (and appropriately protected) records can all result in a fine.

By extension, strong cyber protection must be part of the GDPR preparation process – without taking steps to protect hardware, patch software and implement staff awareness programmes against hacking or phishing, there is a risk of falling short of the expected standard.

For more information on the steps required to successfully comply with GDPR, visit the ICO guidance at tinyurl.com/TE1-12Steps and look at our Tech Essentials guide (details on page 11).

Tech Essentials checklist

Your cut-out-and-keep guide to improving cyber security protection in your business or practice

ALLOCATE RESPONSIBILITIES

- [ ] Management to identify IT vital to the business
- [ ] Decide who is responsible for handling the individual security components

PROTECT YOUR COMPUTERS AND YOUR NETWORK

- [ ] Maintain a firewall
- [ ] Decide if the firewall needs configuring to block certain sites
- [ ] Work out when data was last backed up and implement a regular backing-up programme
- [ ] Test how easily critical data can be restored
- [ ] Decide if you need additional off-site back-up facilities

KEEP YOUR COMPUTERS UP TO DATE

- [ ] Make sure all software used by the business is patched
- [ ] Ensure a regular programme of patching is established and recorded

CONTROL EMPLOYEE ACCESS TO COMPUTERS AND DOCUMENTS

- [ ] Complete an audit of the company's access login IDs, ending any not in use
- [ ] Make sure number of administrators with complete access is kept to a minimum

PROTECT AGAINST VIRUSES

- [ ] Assess the company's anti-virus software needs and adapt systems accordingly
- [ ] Ensure staff are up to speed with the various types of malware (viruses, Trojans and spyware) and how to spot them

EXTEND SECURITY BEYOND THE OFFICE

- [ ] Check all business and personal devices being used outside the company's walls are security protected
- [ ] Ensure all staff working remotely are aware of the dangers and pitfalls – for example when using public wifi

DON'T FORGET DISKS AND DRIVES

- [ ] Instigate a protocol for the use of external hard drives and memory sticks that ensures security of business information and hardware
- [ ] Discourage staff use of these in public places

PLAN FOR THE WORST

- [ ] Identify the most critical elements to be dealt with in the face of a cyber breach
- [ ] Establish a client list that is kept securely and separately from the main IT system in case of system failure caused by a breach
- [ ] Consider creating a full disaster recovery plan in the event of a potential cyber attack (perhaps speaking to a specialist for advice)

EDUCATE YOUR TEAM

- [ ] Work out your business training needs around cyber security – especially social media, emails etc

KEEP RECORDS – AND TEST YOUR SECURITY

- [ ] Implement a system of keeping records to maintain a consistent level of security
- [ ] Regularly test procedures to make sure your security is up to scratch

USEFUL LINKS

ICAEW
The IT Faculty resource centre
icaew.com/cyber
Tech Essentials: GDPR
tinyurl.com/TE4-GDPR
IT Counts blog
ion.icaew.com/itcounts

Government advisory
Cyber Essentials
cyberaware.gov.uk/cyberessentials
Cyber Security Breaches Survey 2017
tinyurl.com/TE4-Survey17
Cyber security guidance for business home page
tinyurl.com/TE4-SecureGuide
Small businesses: what you need to know about cyber security
tinyurl.com/TE4-SmallBusiness
National Cyber Security Strategy 2016-2021
tinyurl.com/TE4-NCSS

Other key bodies
Information Commissioner's Office
ico.org.uk
tinyurl.com/TE4-ICOGuide
Get Safe Online
getsafeonline.org/businesses
National Cyber Security Centre
ncsc.gov.uk
IASME Governance Self-Assessment Preparation Booklet (for Cyber Essentials and GDPR)
A sample questionnaire
tinyurl.com/TE4-IASME
Password checking
howsecureismypassword.net
cyberaware.gov.uk/passwords
Action Fraud
+44 (0)300 123 2040
actionfraud.police.uk

FACULTY INFORMATION

The ICAEW IT Faculty provides products and services to help its members make the best possible use of IT. It represents chartered accountants' IT-related interests and contributes to IT-related public affairs. It also helps those in business to keep up to date with IT issues and developments. As an independent body, the IT Faculty is able to take an objective view and get past the hype which often surrounds IT, leading and shaping debate, challenging common assumptions and clarifying arguments.

ICAEW connects over 147,000 chartered accountants worldwide, providing this community of professionals with the power to build and sustain strong economies. Training, developing and supporting accountants throughout their career, we ensure that they have the expertise and values to meet the needs of tomorrow's businesses.

Our profession is right at the heart of the decisions that will define the future, and we contribute by sharing our knowledge, insight and capabilities with others. That way, we can be sure that we are building robust, accountable and fair economies across the globe.

ICAEW is a member of Chartered Accountants Worldwide (CAW), which brings together 11 chartered accountancy bodies, representing over 1.6m members and students globally.

ICAEW
IT Faculty
Chartered Accountants' Hall
Moorgate Place
London
EC2R 6EA
UK

T +44 (0)20 7920 8481
E itfac@icaew.com
icaew.com/itfac

in search ICAEW IT Faculty
@icaew_ITFaculty
f facebook.com/icaew

Chartered Accountants Worldwide
Member

GAA
Global Accounting Alliance