CYBER CERTIFIED

Making cyber security a key business priority can be achieved by going through an appropriate accreditation process. **Paul Rolison** takes a look at how one in particular, Cyber Essentials, can deliver peace of mind

In addition to delivering products and services, businesses and organisations face a daily grind of living and breathing their regulatory and statutory requirements. With little time and resource left over after all this activity, less pressing matters fall by the wayside. But would you count your cyber security among those matters? Would it be beneficial to put Cyber Essentials (CE) certification on the to-do list when it's not compulsory?

It should be stated that in a growing number of commercial scenarios, CE or CE Plus accreditation is, effectively, mandatory. Various government contracts require certification to be in place, including in supply chains from local government to large and smaller corporations. In these situations, CE certification represents an obvious commercial benefit; being unable to participate in tenders and supply chains could have a significant negative impact on a business's income. There are other incentives to participate: UK organisations signing up to CE get £25,000 cyber insurance cover if their turnover is less than £20m.

Such protection may prove invaluable when you consider the most vulnerable areas for business IT systems. Successful cyber attacks are mainly mounted via email, rogue websites and poorly patched software, while attack methods are often used in combination to achieve the most devastating systems meltdown. The questions asked of organisations during the CE process (see *Steps to certification*, overleaf) enable them to check and confirm the requirements that will help to prevent around 85% of the prevailing attack types (according to GCHQ).

In the case of email, the CE standard expects a number of attachment types to be trapped by the system to prevent the execution of malware code. The configuration required can be a little technical but, as with many aspects of IT, the support team (whether internally or externally) should be able to deal with this and other requirements. Rogue websites can nearly always be rendered harmless with the installation of anti-virus extensions that warn users of a problem where necessary.

Software patching can be tricky, although the vast majority of operating systems and applications have auto-update features. Identifying ones that do not will lead organisations to develop a simple process of regularly checking for updates.

UNDERSTANDING THE SYSTEM

This brings us to the question of whether an organisation has people in place to sort out such updates. There is usually someone who has responsibility for systems in a larger business, but in smaller and medium-sized organisations this is not always clearly defined. As organisations develop and grow, the processes in use (as well as computer systems and applications) also develop and grow.

CE will ask questions about the version of any operating systems in use. It may be the case (at least initially) that the person responsible for the system does not have this level of knowledge – and they may not even be trained in IT. Understanding the operating systems and all the applications in use is key to managing a secure information system.

Perhaps surprisingly, the CE standard only expects organisations to have one written policy in place: a password policy. This will dictate the use and nature of passwords.

However, as organisations going through the process of answering CE questions will see, they would benefit from developing other simple processes for the purpose of keeping the organisation compliant with the CE standard.

These do not need to be onerous, and in many cases can be automated. One example is to assess software that is not in use. PCs, laptops and even Macs come with software that is surplus to requirements, and these can become the source of vulnerabilities.

A simple routine of removing unnecessary software when a device is first installed will be beneficial. Other simple routines can be developed as and when CE questions prompt the need for action. All these new processes together will form the beginning of an information security management system (ISMS).

When it comes to accountability, organisations in the UK must act with reference to the new data protection principle of accountability, which was introduced by the General Data Protection Regulation in 2018. Demonstrating accountability to satisfy this principle will take many forms. For example, a register of personal data used by an organisation demonstrates that this data held and used is understood.

The adoption of the CE standard can help greatly, and it demonstrates that measures have been taken to secure data and systems. The phrase "appropriate technical and organisational measures be taken" appears more than 10 times in the GDPR.

Beyond the benefits of certification itself, just going through the CE process can give an evidence-based check through the system, identifying key elements and confirming that each one has been carefully considered and appropriately configured.

ESSENTIALLY SPEAKING...

While there may be clear and compelling reasons why an organisation will embark upon the journey to achieve CE, there are a number of good practice reasons why every organisation should invest in the standard. Although this article has touched upon both the obvious and not-so-obvious benefits, the most rewarding part must simply be to know that the system has been reviewed, and that there is more confidence in the organisation's level of security than before the CE process was started.

As the word 'essentials' implies, the questions asked during CE accreditation are not in-depth. Many organisations will come out the other side of the process having discovered a lot about their needs: a wake-up call can lead to enlightenment. ●

Paul Rolison
director, Cyber Strategies

GETTY IMAGES

Bedrock for business

ICT manager **Ronnie Ziwa** explains how the Audit Bureau of Circulations approached gaining Cyber Essentials accreditation and what that protection now means to clients

When you mention security to most people, they tend to think of burglar alarms and other physical measures. In the cyber world, security looks rather different; and while the defences are less visible, they're no less important.

Cyber security is a constantly shifting battle and it can be difficult to know which techniques to employ while also ensuring systems remain user-friendly. There's a lot at stake too. According to the *Cost of a Data Breach* study by IBM and the Ponemon Institute, the average financial loss of a cyber attack to a UK organisation was nearly £3m. And the long-term erosion of brand reputation can be even more damaging.

Audit Bureau of Circulations UK is an industry body providing data for the nation's £22bn media sector, and we collect and process lots of client data for print, digital and advertising purposes. It's vital we have high standards of protection in place and can demonstrate that we take the issue seriously, which is why we signed up to Cyber Essentials (CE).

CE is the government-backed, industry-supported scheme to help organisations protect themselves against common cyber attacks. There are two levels: CE and CE Plus. From the outset, the 'Plus' version was our goal. CE Plus requires testing and verification from an independent certifier rather than relying on self-assessment.

We chose to work with business computing experts Ziptech Services to help us through the process. This made the project much more manageable than it would otherwise have been. The agreed approach was to achieve CE first and then immediately move on to CE Plus.

First, we tightened network security by applying stricter policies for all users and computers. We then restructured network traffic in our production environment,

while 'sand-bagging' specific servers so any impact would be minimised if there was a security breach. We required staff using the system to provide more complex passwords, and clear security warnings appear when they're browsing or downloading files online or on email. This requires more effort from users but, as cyber attacks commonly come via malware, ransomware and phishing, it's a small price to secure our infrastructure. And educating users is important – they're a vital part of our defences.

Once all the necessary security policies were applied, and verified by Ziptech, we were accredited for CE. We then moved on to tackle the Plus level. This involved a number of in-depth processes, including tests for all policies we applied, making sure any known vulnerabilities for installed applications were patched within 14 days of receiving a fix from the vendors, and having independent security experts carry out penetration tests on our network.

It was an intense process patching vulnerabilities for many different applications. The nature of our business made the process more complex: we have users who only come into the office once or twice a fortnight. When we ran a scan, we might get results showing all was well one day, but we'd find vulnerabilities that needed patching the next when different auditors were in the office.

We worked for two and a half months scanning for vulnerabilities, deploying patches, then checking to see if they were applied successfully to all machines in our environment. This left us with a healthy dose of paranoia when it comes to cyber security and made us keenly aware of the need to stay ahead of constantly changing cyber threats.

As well as enhancing the security of our infrastructure, achieving CE Plus accreditation also shows potential clients that we take cyber security seriously. Only recently a new client cited the fact we're willing to go the extra mile with our data protection commitments as one of the elements that secured their trust.

As auditors ourselves, we know the benefits of being independently certified. We see CE as a win-win solution that keeps us on our toes and also independently validates the measures we take. ●

Ronnie Ziwa
ICT manager,
Audit Bureau
of Circulations

STEPS TO CERTIFICATION: THE CYBER ESSENTIALS PROCESSES

So, what's the difference between the two cyber certifications? **Cyber Essentials online** is, as the name suggests, an online and self-certifying process. Signing up costs £300 plus VAT. It asks a number of organisation-orientated questions followed by around 40 technical questions. Submitting the answers requires a signed declaration.

Gaining **Cyber Essentials Plus** requires an independent assessment, and generally requires a visit to premises. The process is specified by government and consists of tests relating to emails, website browsing, checking of software patching, anti-malware software configuration and configuration of the firewall facing the internet.

WHY IT'S STILL ESSENTIAL TO GET YOUR CYBER BASICS IN PLACE

An overview from the National Cyber Security Centre

The government has been concerned for some time about widespread cyber threats to organisations across the economy. Low awareness of cyber threats and the relatively easy availability of cheap hacking tools has left many organisations vulnerable; they don't just have to be at risk of a direct, targeted attack. Businesses kept saying they wanted simple advice on how to get basic protections in place. Back in 2013, basic cyber security guidance didn't really exist to help organisations, of all sizes, in any sector, get the basics right.

To fill this gap the government developed Cyber Essentials, which launched in 2014. Through this scheme organisations have been able to demonstrate their commitment to cyber security by achieving a Cyber Essentials certificate. Nearly 40,000 Cyber Essentials certificates have now been awarded, covering businesses of all sizes, charities, local authorities and many other types of organisations, contributing to improving the cyber security of UK PLC. Currently, as far as is known, none of the systems certified by Cyber Essentials has experienced a significant cyber breach.

In 2020 the landscape is slightly different; awareness of cyber threats is much more widespread across the economy. At the heart of government is the National Cyber Security Centre (NCSC), which provides high quality, accessible guidance and support to the public. However, the threat to all organisations of untargeted attacks remains; nearly a third (32%) of businesses suffered a cyber attack in the past 12 months and, despite good progress, many still struggle to get the basics in place. The economy is more online than ever, so Cyber Essentials remains a great first step, especially for smaller businesses.

From April 2020, a strengthened and refreshed scheme will be launched, giving a streamlined user experience. One of the visible changes will be the introduction of expiry dates on certificates, clearly showing the validity of the certification and when recertification is required. To find out more, please visit cyberessentials.ncsc.gov.uk

40K
The number of Cyber Essentials certificates awarded since 2014

32%
How many UK businesses suffered a cyber attack in the past year