DRAGON

Cyber Essentials

Keeping your Business Safe

Cyber Essentials - Keeping your Business Safe

Does anyone rob banks anymore? Recent major data hacks where millions of personal details were stolen from otherwise reputable businesses are a reminder that criminals are targeting your business – but now it's via cyber space.

These cyber criminals are after your money, your data and your intellectual property. When data is stolen from a company you deal with, it breaches your trust in that business. Trust is won slowly, and lost quickly.

While all the details of how these "famous" hacks occurred have not been publicised, typically hackers get into a system through one of many ways:

- Phishing: Your staff accidentally allow hackers in, perhaps by clicking a dodgy link in an email
- Neglect: Operating systems and software quickly get out-of-date, or haven't had the latest security patches updated
- Human error: Accidental loss of data by a member of staff. Like leaving a USB stick or laptop on a train

> *"Almost half of UK firms hit by cyber breach or attack in the past year"*
>
> **SOURCE: DEPARTMENT FOR DIGITAL, CULTURE, MEDIA & SPORT AND NATIONAL CYBER SECURITY CENTRE, 19 APRIL 2017**

And this should make you as nervous as it makes us. We'd rather know exactly what potential problems are lurking, so we can fix them. Wouldn't you?

Cyber-attacks cost organisations like yours thousands of pounds and cause lengthy periods of disruption. Do you have a plan for what you would do if your customer database was stolen, your website was forced offline, or you couldn't access your email or business-critical data?

This is where Cyber Essentials comes into play. It eliminates the guess work and ensures that your business can defend itself against cyber predators. We have. Is it time you did too?

CYBER ESSENTIALS

CYBER ESSENTIALS PLUS

As an added benefit, this will be a big step in getting your business ready **for the new GDPR data laws that start in May**

We're very good at making sure systems are protected and safe, and would hate to see your business suffer the reputational and profit damage that a cyber-attack would involve.

So, let's look at the nitty gritty and how the Cyber Essentials accreditation could help you protect your company from cybercrime now.

Cyber Essentials is a UK government scheme and accreditation scheme. Its primary objective is to make the UK a safer place to conduct online business. Developed together with and supported by industry it fulfils two functions:

1. It ensures organisations implement basic levels of protection against cyber-attacks, within the context of the Government's 10 Steps to Cyber Security.

2. Through the accreditation organisations can demonstrate to customers, investors, insurers and others that they that they take cyber security seriously.

Launched in June 2014, this scheme has become increasingly more relevant for SME's with the new GDPR regulations on the horizon (May 25th 2018) and the need to increase cyber security to comply accordingly.

The scheme identifies fundamental technical security controls an organisation needs to have in place to defend itself against the most common forms of basic cyber-attacks and internet-borne threats.

How it works

Cyber Essentials defines a focused set of five controls which will provide cost effective, basic cyber security for organisations of all sizes. Implemented correctly, they will help you to protect against unskilled internet-based attackers using commodity capabilities:

- **Boundary firewalls and internet gateways**
- **Secure configuration**
- **Access control**
- **Malware protection**
- **Patch management**

The scheme provides organisations with clear guidance on implementation, as well as offering independent certification for those who want it.

The choice is yours

The Assurance Framework, designed in consultation with SMEs to be straightforward and achievable at low cost, offers you two options:

- Cyber Essentials (Standard) - self-assessment
- Cyber Essentials Plus – requiring self-assessment, then followed by an onsite audit involving an assessor to perform a basic vulnerability assessment to ensure security best practices are being performed.

These options give you a choice of the level of assurance you wish to have and the cost of doing so.

The key differentiator for Cyber Essentials PLUS is the inclusion of a technical review of your organisation's workstations. By including this additional phase of testing, the validity of certification increases considerably as it provides evidence of compliance against the following scenarios:

- Can malicious files enter the organisation from the Internet through either web traffic or email messages?
- Should malicious content enter the organisation, how effective are the anti-virus and malware protection mechanisms?
- Should the organisation's protection mechanisms fail, how likely is it that the organisation will be compromised due to failings in the patching of the organisation's workstations?

Cyber Essentials PLUS is a more thorough assessment of your organisation and, as a result, provides greater security assurance. However, it does come at an additional cost, which will factor into your decision-making process.

Ultimately your decision as to which level of certification to implement should be influenced by your organisation's cyber security stance as well as those of your business partners, suppliers and stakeholders.

What it does for you

Strong cyber security enhances your reputation and can win you more business. Cyber Essentials provides a sound foundation of basic security measures that any organisation can implement and build upon. The government believes an organisation's cyber vulnerability can be significantly reduced by implementing these measures.

We see this scheme offering the following advantages:

- It's provides a good balance between providing additional assurance of your company's commitment to implementing cyber security to third parties, while retaining a simple and low-cost mechanism for doing so.
- As the GDPR deadline approaches this scheme acts as a predecessor and a stepping stone to full GDPR compliance on your digital data security.
- Lastly, if your company wants to deal with the MOD or Government, you must have Cyber Essentials as a minimal standard.

Be aware:

- The certification ONLY provides an immediate snapshot of your company's cyber security practices at the time of assessment. Maintaining a robust cyber security stance requires additional measures.
- It does NOT offer a universal remedy that eliminates all cyber security risk; for example, it does not address more advanced, targeted attacks and if your company faces these threat types you will need to implement additional measures into your security strategy.

Business Scope Overview

Assessment and certification can cover the whole of the organisation's IT infrastructure, or a sub-set. Either way, the boundary of the scope must be clearly defined in terms of the business unit managing it, the network boundary and physical location. To achieve the best protection, we strongly recommend that the scope should include the whole IT infrastructure if possible.

The requirements apply to all the devices and software that are within this boundary and that meet the conditions below:

- except incoming network connections from untrusted Internet-connected hosts
- establish user-initiated outbound connections to arbitrary devices via the Internet
- control the flow of data between any of the above devices and the Internet.

> *" Prior to completing the application, I was quietly confident that we would be able to obtain the certification with very little additional work... however I was wrong and it does go into some depth (as you would expect from an assessment developed by CESG, the information security arm of GCGQ)."*
>
> **SOURCE: Alex'sIT Blog, http://www.alexheer.co.uk/it-blog/cyber-essentials-scheme**

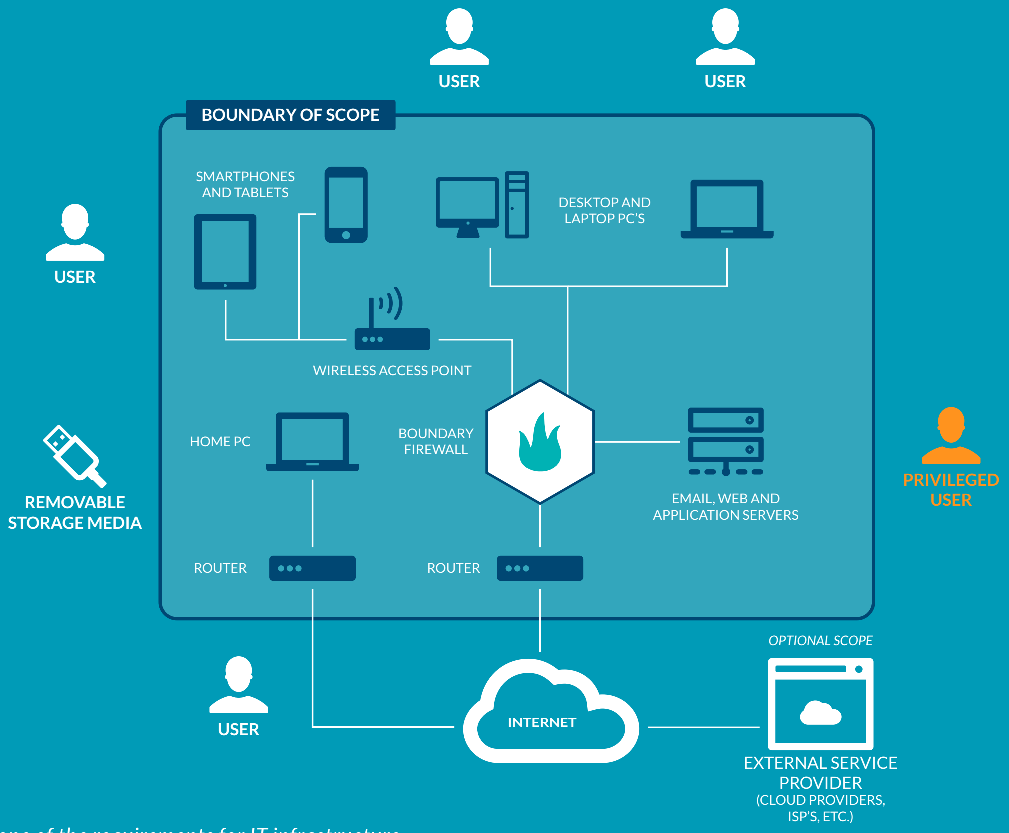

Figure 1: Scope of the requirements for IT infrastructure.

Your next step

The Cyber Essentials documents are FREE to download and any organisation can use them to put essential security controls in place. However, applying for a Cyber Essentials certificate will provide independent assurance that you have the protections correctly in place.

Decide upon the level of protection your organisation needs. We recommend you take the maximum available so you don't leave yourself open to risks.

Lastly, organise the accreditation process and make sure you uphold your cyber protection once you have gained your certification. You will be able to display the Cyber Essentials badge to demonstrate to customers, partners and clients that you take cyber security seriously - boosting reputations and providing a competitive selling point.

What Industry says about Cyber Essentials

“The Information Commissioner’s Office supports the Cyber Essentials scheme and encourages businesses to be assessed against it. Protecting personal data depends on good cyber security, and the threats and challenges are getting ever more sophisticated. All too often organisations fail at the basics. This scheme focuses on the core set of actions that businesses should be taking to protect themselves, their customers, and their brand. Cyber Essentials enables businesses to demonstrate that they are taking action to control the risks”
Christopher Graham, Information Commissioner, Information Commissioner’s Office

“Increasing awareness of the cyber security threat to business is an important issue to the CBI, so we are pleased to be one of the first organisations to take part in the Cyber Essentials scheme. Business leaders will benefit from the access to helpful and authoritative cyber security guidance. Encouraging firms to adopt this scheme is a positive step towards greater awareness of cyber security and more widespread action to manage the risks”
John Cridland, Director General, Confederation of British Industry

“Cyber crime poses a real and growing threat for all businesses and small firms in particular and should not be ignored. Many businesses take steps to protect themselves but the cost of crime can act as a barrier to growth. For example, some businesses refrain from embracing new technology as they fear the repercussions and do not believe they will get adequate protection from crime. In the face of an ever increasing threat of cyber attacks, the FSB supports the Cyber Essentials scheme as an additional and important tool, designed to help reduce the risk to small firms and improve the resilience of the sector”
Mike Cherry, National Policy Chairman, Federation of Small Businesses

“IRM regularly sees the damaging commercial and personal consequences of weak cyber security. As an early adopter of Cyber Essentials ourselves, we’re keen that as many organisations as possible start implementing its principles at the earliest opportunity.”
Jeremy Harrison Interim Chief Executive, Institute of Risk Management

For proven, trusted IT systems
support to keep your business
trading profitably

Dragon Information Systems Ltd
6 Bassett Court, Newport Pagnell, Bucks MK16 0JN
Tel: 01908 613 080 | helpdesk@dragon-is.com | www.dragon-is.com