Cyber Essentials
A Guide to the Scheme

CYBER ESSENTIALS

Security controls to help prevent around 80% of cyber attacks.

Essential security - Cyber Essentials

Good cyber security should be built on firm foundations. As the sermon goes, you can't build your castle on sand and expect it not to sink.

Any organisation can be targeted by cyber criminals. However, SMEs (small and medium-sized enterprises) are at a higher risk of being hacked than their larger counterparts. Criminal hackers expect larger organisations to be better protected, whereas SMEs often lack the resources to protect themselves against evolving cyber threats.

But before spending money on the latest security tools or consultants, consider what you could do with the resources you already have.

The risk to small businesses

Cyber Essentials

The Zurich SME Risk Index makes interesting reading. It revealed that almost one in six SMEs fell victim to a cyber attack within a 12-month period. Of the businesses affected, more than a fifth reported that it cost them more than £10,000, and one in ten said it cost more than £50,000.

On the flip side, the robustness of cyber security is now a genuine criterion for winning and maintaining business contracts. A quarter of medium-sized businesses (50–249 employees) and one in ten small business reported that they have been directly asked by a prospective customer about what cyber security measures they have in place.

Cyber Essentials – the cyber security starting point for all SMEs

Most criminal hackers aren't state-sponsored agencies or activists looking for high-profile targets, and they don't spend countless hours staking out and researching their targets.

Instead, they're more opportunistic, looking for poorly-protected targets. Just like an organised house burglar might send out scouts looking for signs of poorly-safeguarded properties, the modern cyber criminal will send out phishing emails or network scans looking for vulnerable systems.

In a single day they can assess millions of potential targets. Attacks often target as many devices, services or users as possible using the 'openness' of the Internet.

Security controls to help prevent 80% of attacks

The Cyber Essentials scheme is a world-leading, cost-effective assurance mechanism for companies of all sizes to help demonstrate to customers and other stakeholders that the most important cyber security controls have been implemented. The scheme provides five security controls that, according to the UK government, could prevent "around 80% of cyber attacks".

The Assurance Framework, leading to the awarding of Cyber Essentials and Cyber Essentials Plus certificates for organisations, has been designed in consultation with SMEs to be light-touch and achievable at low cost.

The Cyber Essentials scheme provides five security controls, that, according to the UK government, could prevent “around 80% of cyber attacks”.

Whether or not you achieve certification to the scheme, these controls provide the basic level of protection that you need to implement in your organisation to protect it from the vast majority of cyber attacks, allowing you to focus instead on your core business objectives.

Properly implemented cyber security has the additional advantage of driving business efficiency throughout the organisation, saving money and improving productivity.

Cyber Essentials certification can also reduce insurance premiums. A government report in March 2015 (UK cyber security: the role of insurance in managing and mitigating the risk) found that the majority of insurers believe “that Cyber Essentials would provide a valuable signal of reduced risk when underwriting cyber insurance for SMEs, allowing them to use a reduced question set and informing their decisions to underwrite”, and that “participating insurers operating in the SME insurance sector have agreed to build reference to the Cyber Essentials standard into their cyber insurance applications, and will look to simplify the application where accreditation has been achieved by the applicant”.

The benefits of achieving Cyber Essentials certification

Protected against approximately 80% of cyber attacks Implementing the five controls correctly will help you protect your organisation.

Demonstrate security and help secure the supply chain Achieving Cyber Essentials certification will help you demonstrate your commitment to protecting both your own data and that of your customers and suppliers.

Increase chances of securing business Cyber Essentials certification will help boost your reputation and give you a better chance of winning contracts.

Drive business efficiency You will be able to focus on your core business objectives knowing that you are protected from the vast majority of common cyber attacks.

Work with the UK government and MoD Cyber Essentials will give you the opportunity to work with the UK government and Cyber Essentials Plus will give you the opportunity to work with the Ministry of Defence.

Reduce cyber insurance premiums Cyber insurance agencies look more favourably on organisations that have acheived Cyber Essentials certification.

Cyber Essentials

What are the five controls? If a cyber-criminal is explicitly targeting your organisation using bespoke tools they have created to gain access, then Cyber Essentials will perhaps not be adequate to protect your systems. But for the more common and freely available hacking tools, it is an excellent starting point to help keep your head below the parapet. It covers the following key areas:

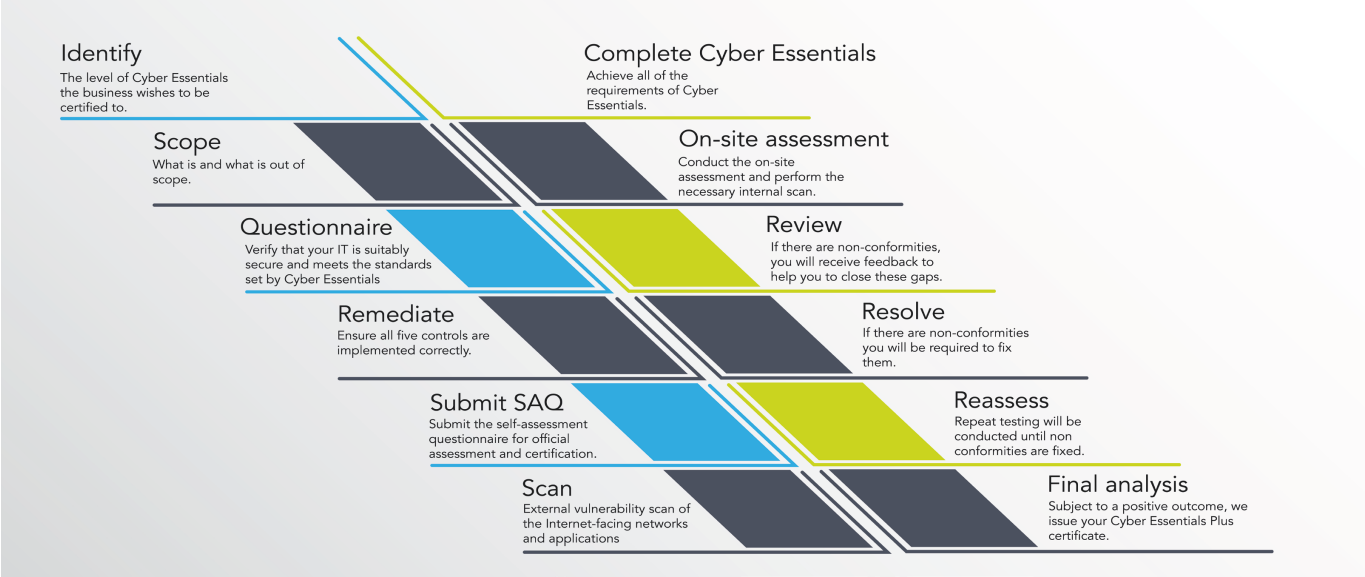
What is in scope and what is not. Assessment and certification can cover the whole IT infrastructure, or a sub-set. Whichever scenario, the boundary of the scope must be clearly defined in terms of the function managing it, the network boundary and physical location. The requirements apply to all the devices and software that meet the following conditions: • Accept incoming network connections from untrusted Internet-connected hosts; • Establish user-initiated outbound connections to devices via the Internet; • Control the flow of data between any of the above devices and the Internet.

In addition to mobile or remote devices owned by the organisation, user-owned devices which access organisational data or services are in scope.

Wireless devices (including wireless access points) are also in scope if they can communicate with other devices via the Internet. And if it is practicable to apply the requirements to cloud services then these services are within the boundary of scope.

Commercial web applications created by development companies (rather than in-house developers) and which are publicly accessible from the Internet are also in scope by default.

The process for completing Cyber Essentials and Cyber Essentials Plus.



Secure configuration

Applies to: Email, web and application servers; desktop computers; laptops; tablets; mobile phones; firewalls; routers.

Objective: Confirm that computers and network devices are properly configured to reduce the level of inherent vulnerabilities and provide only the services required to fulfil their role.

Computers and network device requirements:

The organisation must routinely: • Remove and disable unnecessary user accounts; • Change any default or guessable account passwords to something non- obvious; • Remove or disable unnecessary software; • Disable any auto-run feature that allows file execution without user authorisation; and • Authenticate users before allowing Internet-based access to commercially or personally sensitive data, or data critical to the running of the organisation.

Password-based authentication requirements: • Protect against brute-force password guessing, by using at least one of the following methods: limit attempts, or the number of guesses allowed in a time period. • Set a minimum password length of at least eight characters but not set a maximum password length. • Change passwords promptly when the applicant knows or suspects they have been compromised. • Have a password policy that informs users of best practices.

Requirements for IT Infrastructure Here we list the specific requirements under five technical control areas: • Secure configuration • Firewalls • User access control • Patch management • Malware protection

User access control

Applies to: Email, web and application servers; desktop computers; laptops; tablets; mobile phones.

Objective: Confirm that user accounts are assigned to authorised individuals only, and provide access to only those applications, computers and networks required for the user to perform their role.

Requirements:

The organisation must be in control of its user accounts and the access privileges granted to each user account. It must also understand how user accounts authenticate and control the strength of that authentication. • Authenticate users before granting access to applications or devices, using unique credentials. • Remove or disable user accounts when no longer required. • Implement two-factor authentication, where available. • Use administrative accounts to perform administrative activities only. • Remove or disable special access privileges when no longer required.

Firewalls

Applies to: Boundary firewalls; desktop computers; laptops; routers; servers.

Objective: Confirm that only safe and essential network services can be accessed from the Internet.

Requirements:

Every device that is in scope must be secured by a correctly configured firewall (or equivalent network device). For all firewalls (or equivalent network devices), the organisation must routinely: • Change any default administrative password to an alternative using best practices – or disable remote administrative access entirely; • Prevent access to the administrative interface from the Internet, unless there is a clear and documented business need and the interface is protected by one of the following controls: • A second authentication factor, such as a one-time token; or • An IP whitelist that limits access to a small range of trusted addresses. • Block unauthenticated inbound connections by default; • Ensure inbound firewall rules are approved and documented by an authorised individual; the business need must be included in the documentation; and • Remove or disable permissive firewall rules quickly when they are no longer needed. Use a host-based firewall on devices that are used on untrusted networks, such as public Wi-Fi hotspots.

Patch management

Applies to: Web, email and application servers; desktop computers; laptops; tablets; mobile phones; firewalls; routers.

Objective: Confirm that devices and software are not vulnerable to known security issues for which fixes are available.

Requirements:

The organisation must keep all its software up to date. Software must be: • Licensed and supported; • Removed from devices when no longer supported; and • Patched within 14 days of an update being released, where the patch fixes a vulnerability with a severity the vendor describes as ‘critical’ or ‘high risk’.

If your software vendor uses different terms to the CVSS (Common Vulnerability Scoring System). For the purposes of the Cyber Essentials scheme, ‘critical’ or ‘high risk’ vulnerabilities are as follows: • Attack vector: network only • Attack complexity: low only • Privileges required: none only • User interaction: none only • Exploit code maturity: functional or high • Report confidence: confirmed or high

Malware

Applies to: desktop computers; laptop computers; tablets; mobile phones.

Objective: Restrict execution of known malware and untrusted software, to prevent harmful code from causing damage or accessing sensitive data.

Requirements:

The organisation must use at least one of the three approaches listed below:

Anti-malware software • The software must be kept up to date, with signature files updated at least daily. • The software must be configured to scan files automatically upon access. This includes when files are downloaded and opened, and when they are accessed from a network folder. • The software must scan web pages automatically when they are accessed through a web browser. • The software must prevent connections to malicious websites on the Internet.

Application whitelisting • Only approved applications are allowed to execute on devices. The organisation must: actively approve such applications before deploying them to devices; and maintain a current list of approved applications.

Application sandboxing • All code of unknown origin must be run within a ‘sandbox’ that prevents access to other resources unless permission is explicitly granted by the user.