5 Cyber Essentials key controls

Boundary firewalls and internet gateways – good set up of devices designed to prevent unauthorised access to or from private networks

Secure configuration – systems are configured in the most secure way

Access control – only those who should have access to systems have access, and at the appropriate level

Malware protection – virus and malware protection is installed and up-to-date

Patch management – the latest supported version of applications is used and all necessary patches have been applied

Further information

The Cyber Essentials free download and list of Accreditation Bodies can be found on the Cyber Essentials web (located on Cyber Streetwise):

www.cyberstreetwise.com/cyberessentials

Guidance to help maintain cyber security defences

10 Steps to Cyber Security available from GOV.UK at www.gov.uk/government/publications/ cyber-risk-management-a-board-level- responsibility

What you need to know about Cyber Security available from GOV.UK at www.gov.uk/government/publications/ cyber-security-what-small-businesses- need-to-know

HM Government

HM Government

CYBER ESSENTIALS

CYBER ESSENTIALS PLUS

Protect your business against cyber threats

Cyber Essentials

Cyber Essentials is a new Government-backed and industry supported scheme to help businesses protect themselves against cyber threats.

As reliance on internet technologies increases, so do the opportunities for criminals and hackers to commit fraud, industrial espionage or the theft of intellectual property. Cyber Essentials defines a set of five key security controls (see overleaf) which, when properly implemented, will better protect businesses, small and large, from attacks using software and techniques which are freely available on the open internet.

How it works

Designed to be light-touch and achievable at low cost, the Cyber Essentials questionnaire is free for businesses to download, with the option of paying for independent assessment and certification.

Cyber Essentials or Cyber Essentials Plus?

Cyber Essentials offers two levels of certification:

Cyber Essentials - for a small fee, this basic level of certification is awarded on the basis of a completed self-assessment questionnaire, which is then verified by an independent Certification Body.

Cyber Essentials Plus - offers - at additional cost - a higher level of assurance, with the Certification Body testing that the five key controls are working in practice by simulating basic hacking and phishing attacks.

Why should you consider Cyber Essentials?

- You can prevent many attacks which use freely available software and techniques by implementing the Cyber Essentials five controls
- You can identify areas for improvement, even if your company has a proven track record of good security, by going through the assessment
- Your business can display the Cyber Essentials badge and demonstrate that it takes cyber security seriously by adhering to a widely-endorsed standard

Getting assessed

If you'd like to get your organisation assessed, one of the Cyber Essentials Accreditation Bodies (list available on www.cesg.gov.uk/servicecatalogue/cyber-essentials.aspx or Cyber Streetwise) can discuss your requirements and identify a Certification Body to carry out the assessment.

Next steps

No measures, however well implemented, can provide 100% protection from internet-based attack. Cyber Essentials is a good place to start but needs to be viewed by businesses as the start of a journey. Cyber Essentials offers a snapshot of the cyber security practices of the organisation at the time of certification – the next step is for organisations to sustain these levels of security as part of an ongoing risk management approach.

"Cyber Essentials gave us the opportunity to undertake a thorough review of a sub-set of our technical security controls. As a result, we strengthened our firewall rules but, equally importantly, Cyber Essentials helped us identify weaknesses in the processes that managed our technology."

Colin Robbins, Technical Director, Nexor