HM Government

CYBER ESSENTIALS

Cyber Essentials Scheme

Summary

June 2014

Introduction

The Cyber Essentials scheme has been developed by Government and industry to fulfil two functions. It provides a clear statement of the basic controls all organisations should implement to mitigate the risk from common internet based threats, within the context of the Government's 10 Steps to Cyber Security. And through the Assurance Framework it offers a mechanism for organisations to demonstrate to customers, investors, insurers and others that they have taken these essential precautions.

Cyber Essentials offers a sound foundation of basic hygiene measures that all types of organisations can implement and potentially build upon. Government believes that implementing these measures can significantly reduce an organisation's vulnerability. However, it does not offer a silver bullet to remove all cyber security risk; for example, it is not designed to address more advanced, targeted attacks and hence organisations facing these threats will need to implement additional measures as part of their security strategy. What Cyber Essentials does do is define a focused set of controls which will provide cost-effective, basic cyber security for organisations of all sizes.

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 two options give organisations a choice over the level of assurance they wish to gain and the cost of doing so. It is important to recognise that certification only provides a snapshot of the cyber security practices of the organisation at the time of assessment, while maintaining a robust cyber security stance requires additional measures such as a sound risk management approach, as well as on-going updates to the Cyber Essentials control themes, such as patching. But we believe this scheme offers the right balance between providing additional assurance of an organisation's commitment to implementing cyber security to third parties, while retaining a simple and low cost mechanism for doing so.

Addressing the Threat

Cyber Essentials defines a set of controls which, when properly implemented, will provide organisations with basic protection from the most prevalent forms of threats coming from the Internet. In particular, it focuses on threats which require low levels of attacker skill, and which are widely available online.

Risk management is the fundamental starting point for organisations to take action to protect their information. However, given the nature of the threat, Government believes that action should begin with a core set of security controls which all organisations – large and small – should implement. Cyber Essentials defines what these controls are.

Background

In 2012 Government launched its 10 Steps to Cyber Security and subsequently Small Businesses: What you need to know about cyber security guidance to encourage organisations to consider whether they were managing their cyber risks. Government emphasised the need for company Boards and senior executives to take ownership of these risks and enshrine them within their overall corporate risk management regime. These initiatives continue to gain traction. However, government analysis of continuing attacks and feedback from industry vulnerability testers has identified that a number of security controls are still not being applied, leaving organisations vulnerable to threat actors with low levels of technical capability.

We view the adoption of an organisational standard for cyber security as the next stage on from the 10 Steps to Cyber Security guidance. This will enable organisations, and their customers and partners, to have greater confidence in their ability to reduce the risk posed by threat actors with low levels of technical capability, independently tested where necessary.

The Cyber Essentials Scheme follows on from a call for evidence on a preferred organisational standard in cyber security carried out by Government together with industry, which concluded in November 2013. Information about this call for evidence, including the outcome document, can be found here.

The feedback we received from industry through the call for evidence was that none of the existing organisational standards for cyber security met our requirements, but that industry was keen to help us develop something new.

Government has therefore worked with industry to develop new requirements. This is the Cyber Essentials Scheme, which focuses on basic cyber hygiene. Information Assurance for Small & Medium Enterprises, (IASME), Information Security Forum (ISF), and the British Standards Institution (BSI) have collaborated on the project. Other organisations, including professional bodies and individual businesses, have provided technical advice.

Scope

The Cyber Essentials Scheme covers the basics of cyber security in an organisation's enterprise or corporate IT system. Implementation of these controls can significantly reduce the risk of prevalent but unskilled cyber-attack. For many organisations, especially those with significant information assets or who are exposed to a wider range of threats, Cyber Essentials will become a practical component of a wider ranging cyber security posture – for example, as described in the Government's '10 Steps to Cyber Security' and 'Cyber Security: what small businesses need to know'.

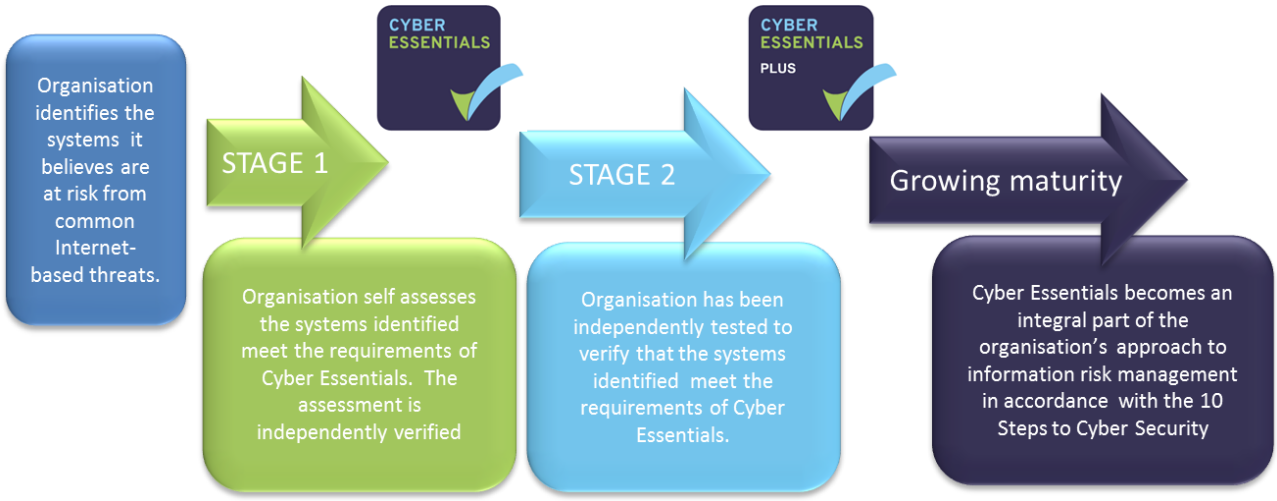

Figure 1 - Cyber Essentials Scheme: overview

The Scheme Requirements Document focuses on Internet-originated attacks against an organisation's IT system. Many organisations will have particular additional services, e.g. web applications, that will require additional and specific controls beyond those provided by Cyber Essentials. Cyber Essentials concentrates on five key controls. These are:

1. **Boundary firewalls and internet gateways** - these are devices designed to prevent unauthorised access to or from private networks, but good setup of these devices either in hardware or software form is important for them to be fully effective.
2. **Secure configuration** – ensuring that systems are configured in the most secure way for the needs of the organisation
3. **Access control** – Ensuring only those who should have access to systems to have access and at the appropriate level.
4. **Malware protection** – ensuring that virus and malware protection is installed and is it up to date
5. **Patch management** – ensuring the latest supported version of applications is used and all the necessary patches supplied by the vendor been applied.

Assurance Framework

As stories of organisations exposing customers' information to cyber threats continue to create headlines in the media, it is becoming increasingly important for organisations to not only maintain a robust cyber security stance but also demonstrate this to clients. The Assurance Framework is designed to provide a simple means for third parties to distinguish between organisations that are implementing basic cyber security controls from those that are not. This can be used in a number of ways; an organisation may undergo certification to mark them out from their competitors; they may require certification from partners where contractual relationships expose them to wider cyber risk (for example where information is shared); and insurers, investors and auditors may take certification into account when assessing an organisation's risk profile.

The two levels of certification, Cyber Essentials, and Cyber Essentials Plus are set out in Figure 1 above.

- **Cyber Essentials** certification is awarded on the basis of a verified self-assessment. An organisation undertakes their own assessment of their implementation of the Cyber Essentials control themes via a questionnaire, which is approved by a senior executive such as the CEO. This questionnaire is then verified by an independent Certification Body to assess whether an appropriate standard has been achieved, and certification can be awarded. This option offers a basic level of assurance and can be achieved at low cost.

- **Cyber Essentials Plus** offers a higher level of assurance through the external testing of the organisation's cyber security approach. Given the more resource intensive nature of this process, we anticipate that Cyber Essentials Plus will cost more than the foundation Cyber Essentials certification.

On successful completion a certificate will be awarded. Organisations who receive a certificate will be able to display the appropriate Cyber Essentials or Cyber Essentials Plus badge.

Next steps

Organisations wishing to be assessed should contact one of the Cyber Essentials Accreditation Bodies to discuss their requirements and identify a Certification Body.

For further information about how to become certified, see: www.cyberessentials.org.uk

If you would like to become a Certification Body, see www.cyberessentials.org.uk where links to the Accreditation Bodies can be found.

If you would like to become an Accreditation Body, please contact cyberessentials@cesg.gsi.gov.uk.

Questions about the scheme?

1. Who is 'Cyber Essentials' for?

Cyber Essentials is applicable to all organisations, of all sizes, and in all sectors. We encourage all organisations to look at the requirements and to adopt them. This is not limited to companies in the private sector, but is applicable to universities, charities, public sector and not-for-profit organisations.

2. What are the benefits of the scheme?

The Cyber Essentials scheme provides organisations with clarity on what essential security controls they need to have in place to reduce the risk posed by threats on the Internet with low levels of technical capability. Organisations that are good at cyber security can make this a selling point – demonstrating to their customers through the Cyber Essentials badge that they take cyber security seriously.

3. When can I apply to this scheme?

The scheme is open now and is available to all organisations. Those interested in assessment should in the first instance contact one of the Accreditation Bodies to identify a suitable Certification Body.

4. How much will it cost to be certified?

Our intention is that the scheme will be affordable to the greatest possible number of organisations. Costs will be set by the individual Certification Bodies who will work in competition with each other, allowing market forces to set rates. The cost will depend on size of your organisation and the level of rigour you need to demonstrate. The Assurance Framework proposes two stages reflecting different levels of assurance: Cyber Essentials and Cyber Essentials Plus.

5. How will I show that I have been certified?

Organisations that have successfully been assessed against the scheme will be able to use the appropriate Cyber Essentials badge to publicise this fact. Being able to advertise that you have met a Government approved cyber security scheme will give you an edge over competitors in the same market.

6. Will there be a time limit on the badge?

The assessment process is a 'snap shot' in time and it can only be sure to be effective on the day of assessment, similar to an MoT on a car. As with the MoT the car will not remain roadworthy without regular maintenance. New vulnerabilities are continually being identified. We therefore recommend that organisations maintain the principles of the Scheme on an on-going basis (for example, ensuring that patching always occurs in a timely fashion and that malware protection is kept up to date) and not just prepare for assessment. As a minimum, to retain the badge organisations must recertify at least once a year.

7. My organisation already complies with a standard in cyber or information security – for example, ISO 27001. Am I supposed to get us assessed against Cyber Essentials as well?

Yes. You can gain the badge in addition to other schemes. The process of meeting the requirements of other standards may have included work which meets or partially meets the Cyber Essentials Requirements. Your Certification Body will be able to advise you

further. It is intended that compliance with Cyber Essentials will add value to the majority of organisations and demonstrate to customers, partners and stakeholders that you take information security seriously.

8. Is implementing just the Cyber Essentials controls enough?

Cyber Essentials aims to describe the small number of fundamental mitigations that will stop the majority of internet based cyber-attacks to your IT system. It is important that you think about your own organisation and risk as set out in the '10 Steps to Cyber Security' guidance to determine if implementing the Cyber Essentials alone is enough for you. Many organisations will need to have in place far more controls and procedures to manage the risks they face. Cyber Essentials can be seen as a first, vital step.

9. Why does the profile focus on five controls and how were they chosen?

CESG (the information security arm of GCHQ) has carried out an analysis of successful Cyber Attacks on a wide range of organisations. This analysis has helped identify the basic technical controls which most effectively mitigate cyber attacks by unsophisticated attackers using attack tools that are widely available on the internet. Cyber Essentials comprises the core actions necessary to mitigate the majority of these threats.

10. Where does Cyber Essentials fit with Cyber Streetwise, Get Safe Online and existing Government guidance on cyber security?

These initiatives provide advice and guidance for the general public and SMEs. Links to government guidance are provided above, and Cyber Streetwise can be accessed here for advice on protecting your business. 10 Steps to Cyber Security is designed to assist boards in assessing whether their approach to corporate risk is taking adequate account of cyber security.

11. Will this be mandated by government?

Government will require all suppliers bidding for certain contracts which are assessed as higher risk to be Cyber Essentials certified. This is likely to include ICT and personal and sensitive information handling contracts.

12. I have a secure website; do I still need to use Cyber Essentials?

A secure website may provide a secure link between you and your customer. Cyber Essentials aims to protect the data once it is stored within your systems. Again, whether you need certification by the scheme or not is your business decision.

13. Will Cyber Essentials stop me getting hacked?

Cyber Essentials offers a sound foundation of basic hygiene measures that all types of organisations can implement and potentially build upon. We believe that implementing these measures can significantly reduce an organisation's vulnerability. However, it does not offer a silver bullet to remove all cyber security risk; for example, it is not designed to address more advanced, targeted attacks and hence organisations facing these threats will need to implement additional measures as part of their security strategy.

14. I believe my company has the skills to carry out assessment, how do I get a licence to do so?

The Assurance Framework accompanying this document contains details of how you can find out more about this.

15. What do I need to do if my service is outsourced?
What may be in or out of scope of certification is detailed in the Assurance Framework.

This publication is also available on our website at www.gov.uk

Any enquiries regarding this publication should be sent to:

Department for Business, Innovation and Skills
1 Victoria Street
London SW1H 0ET
Tel: 020 7215 5000

If you require this publication in an alternative format, email enquiries@bis.gsi.gov.uk, or call 020 7215 5000.

BIS/14/696