SLAUGHTER AND MAY

BRIEFING
AUGUST 2014

Reactions to the UK's Cyber Essentials Scheme

The formal launch of the Government's Cyber Essentials scheme took place on 5 June 2014, and a number of organisations (including Barclays, who spoke at the launch) have already applied for the new Cyber Essentials Award. In this article Rob Sumroy and Natalie Donovan look at what the scheme covers, and how some organisations are responding to its launch.

WHAT DOES IT COVER?

Cyber Essentials is "a government-backed, industry supported scheme to help organisations protect themselves against common cyber attacks[1]". Its launch follows the Government's consultation last year on the requirements for a preferred standard for cyber security *(see background to the scheme box)* and incorporates the output of work between Government and industry following that consultation.

It has been designed to satisfy two main goals:

Guidance: Firstly, 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'" guidance.[2] The requirements document, which was developed in collaboration with industry partners,[3] identifies basic technical security measures organisations should have in place. It focuses on five key controls, namely:

i. boundary firewalls and internet gateways;
ii. secure configuration;
iii. user access controls;
iv. malware protection; and
v. patch management.

BACKGROUND TO THE SCHEME

- The Cyber Essential scheme is a key objective of the Government's National Cyber Security Strategy.
- The Government saw the adoption of an organisational standard for cyber security as the next step on from its 10 steps to Cyber Security Guide (published in September 2012).
- In March 2013 it instigated a call for evidence on a preferred organisational standard.
- The results (released in November 2013) suggested that current standards did not fully meet the requirements of participants, but that industry would work with the Government to draw up a new standard, based on the ISO27000-series and focusing on basic cyber hygiene.
- The resulting requirements have been embedded into the Cyber Essentials Scheme.

1 https://www.gov.uk/government/publications/cyber-essentials-scheme-overview
2 Cyber Essentials Scheme Summary – June 2014 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/317480/Cyber_Essentials_Summary.pdf
3 Including the Information Security Forum (ISF) and British Standards Institution (BSI)

It discusses simple protections around them, for example changing default passwords, disabling or removing unnecessary user accounts and software, restricting special access privileges, putting in place clear approval processes around account creation and keeping all software (including anti-malware software and patches) up to date. The information provided is very basic, although this is not necessarily surprising – partly as it has been designed to ensure it is accessible to SMEs (although the requirements document does state the control themes are relevant to organisations of all sizes) and partly as the aim of the requirements is to defend against common forms of internet based cyber attacks using widely accessible tools. It is not, therefore, designed to address more advanced, targeted attacks. However, it does provide more information on where to obtain advice and where these requirements are covered in more detailed standards and guidance (such as ISO 27001/2).

Certification: Its second goal is to offer a mechanism for an organisation to demonstrate (for example to potential customers) that it takes cyber security seriously. This mechanism, the 'Assurance Framework', allows organisations to apply to be certified. Again, it has been developed in consultation with SMEs to be 'light touch' and achievable at low cost. There will be two stages or levels of compliance – Cyber Essentials and Cyber Essentials Plus[4]:

- Stage 1: Cyber Essentials certification is awarded on the basis of a verified self assessment. An organisation will respond to the Cyber Essentials questionnaire, declaring its compliance with the Cyber Essential requirements. The declaration (signed by an organisation's CEO or equivalent) is then sent to an independent Certification Body for verification.

- Stage 2: Cyber Essentials Plus certification encompasses the same control themes as Cyber Essentials, but offers more assurance through the use of an independent testing regime, based on vulnerability testing of the relevant system(s) (which the organisation will scope).

Interestingly, this has changed from the three tiers (bronze, silver and gold) originally suggested when the draft framework was issued for comment in April of this year.

Guidance states that organisations will need to recertify once a year, or more frequently as necessary to meet specific procurement or customer requirements[5].

HOW WILL CERTIFICATION WORK?

The Government has established a 'scalable framework of Accreditation and Certification Bodies'[6]. It appoints Accreditation Bodies (such as CREST[7] and IASME[8]) who in turn appoint Certification Bodies. A number of Certification Bodies already exist. For example, the CREST website lists some,[9] such as BT Security, HP and Deloitte.

From 1 July 2014 it will also be possible to verify an organisation's Cyber Essentials certificate online, using the relevant certificate reference number.[10]

4 Although information on cyberessentials.org states that future levels are planned
5 Cyber Essentials Scheme Assurance Framework June 2014 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/317482/Cyber_Essentials_Assurance_Framework.pdf
6 As above
7 See http://www.cyberessentials.org/
8 IASME (Information Assurance for SMEs) are an accreditation body for cyber essentials https://www.iasme.co.uk/index.php/cyberessentialsprofile and have also developed their own information assurance standard
9 http://www.cyberessentials.org/companies/index.html
10 http://www.cyberessentials.org/verify-a-certificate/index.html

WHAT ARE THE COSTS INVOLVED?

The costs of certification are not set by the Government, but will be left to market forces. By way of example, SME focused IASME is planning to offer self-assessment against the Cyber Essentials Scheme at a cost of £300, with an 'assisted self-assessment' service expected to cost £1,100. Costs for third party independent assessment (which seems to cover Cyber Essentials Plus) will vary according to the size of the business, its complexity and its risk profile. IASME's website does provide some cost guidelines for organisations. These range from £2,500 - £10,000, depending on the size of the organisation (with the largest category listed having between 100-250 employees). The estimated costs for annual accreditation renewal are slightly lower, ranging from £1,000 to £4,000.

SMEs struggling to fund compliance or certification can apply for a Government grant to assist.[11]

WHAT DO ORGANISATIONS THINK?

We have carried out a survey across a broad sample of our client base to gauge their response to the launch and discover whether their organisations are currently considering certification. Many of these are large corporates or multi-national organisations. Interestingly very few are currently planning to certify, and those that are plan to self-certify at this stage. Instead, many respondents preferred other, more detailed, standards such as ISO 27001/2 which they felt were more relevant to their business, and still covered the points raised in the Cyber Essentials requirements. It will be interesting to see if this view changes if there is a high adoption rate, and how the government (who have pledged to require certain potential suppliers to be certified from 1 October 2014)[12] will manage bidders in its procurements who are not formally certified, but whose controls satisfy the requirements.

Many also suggested that the scheme currently lacked proper marketing or promotion. While most were aware of the scheme to some degree, not all had heard of it (despite carrying out work on cyber security) and some did not realise it had formally launched. Others were only aware of it from secondary sources (such as the ICO, who recently welcomed the scheme, stating "protecting personal data depends on good cyber security"[13]) rather than from any specific government advertising.

A number of respondents thought it would be more appropriate for SMEs than for their (larger) organisation. That said, some did like the simplicity of having one framework highlighting the five most important controls that are applicable to all organisations and felt this provided a clear focus for information security. One government contractor commented that it was "a great initiative by UK government" as it allowed organisations to work to one framework for all of the UK government's requirements and would provide greater confidence to its customers.

COMMENT:

The scheme is a key objective of the Government's National Cyber Security Strategy, which it hopes will be widely adopted by organisations of all sizes. It has tried to design a scheme which strikes the right balance: providing assurance of an organisation's commitment to implementing cyber security to third parties, while ensuring the scheme is simple and low cost and therefore accessible to all. This balance can be difficult to achieve, and

11 https://vouchers.innovateuk.org/cyber-security

12 The Government announced at the launch that, from 1 October 2014, it will require all suppliers bidding for certain personal and sensitive information handling contracts to be Cyber Essentials certified

13 http://ico.org.uk/news/current_topics/cyber-essentials

inevitably some larger organisations may feel that existing standards, and their current security practices which comply with them are already more sophisticated and developed than the basic controls covered by the Cyber Essentials scheme. However, it may provide a useful focus for those organisations with limited security budgets, or who want to measure their current practices against an independent benchmark.

It is not yet clear whether the scheme will catch on, and few of the organisation we spoke to currently see it as the marketing tool the Government hopes it will become. However, backing from association's such as the BIBA[14] and the International Underwriting Association, as well as corporations such as Marsh and Swiss Re will help encourage adoption, as should the Government's pledge to require certain potential suppliers to be certified.

Written by Rob Sumroy and Natalie Donovan of Slaughter and May's Technology Group

This article was first published in e-commercelaw&policy July 2014 (Volume 16, Issue 7)

[14] British Insurance Brokers' Association

ROB SUMROY
T +44 (0)20 7090 4032
E rob.sumroy@slaughterandmay.com

NATALIE DONOVAN
T +44 (0)20 7090 4058
E natalie.donovan@slaughterandmay.com