The Bare Essentials

Change is afoot in the Cyber Essentials scheme, Anne W explains what is happening

In November 2017 the NCSC launched the new Cyber Essentials microsite. At the time I blogged that "*The NCSC is committed to nurturing the Cyber Essentials scheme towards fulfilling its role in helping to make the UK one of the safest places to live and do business on-line*".

This remains as true today as it did 18 months ago, but as part of this commitment, we are now actively pursuing some of the changes I hinted at back then. This blog aims to bring you up to date with what's happening in this space.

First things first

Before I go into detail on the changes coming to the scheme, let me start by answering a few of the questions that came up a lot during CyberUK this year.

Does the government believe Cyber Essentials still relevant?

In a nutshell, yes we believe it is. Since it's launch in 2014 the NCSC, through a network of over 200 Certification Bodies has issued almost 30,000 certificates. And whilst we can't prove a direct correlation, as far as we are aware, none of the systems certified has experienced a significant cyber security breach.

So the NCSC isn't killing it off then?

Absolutely not. In its National Cyber Security Strategy, the government specifically calls out its commitment to the scheme by saying:

> **CYBER ESSENTIALS**
>
> **The Cyber Essentials scheme was developed to show organisations how to protect themselves against low-level "commodity threat." It lists five technical controls (access control; boundary firewalls and Internet gateways; malware protection; patch management and secure configuration) that organisations should have in place.**
>
> **The vast majority of cyber attacks use relatively simple methods which exploit basic vulnerabilities in software and computer systems. There are tools and techniques openly available on the Internet which enable even low-skill actors to exploit these vulnerabilities. Properly implementing the Cyber Essentials scheme will protect against the vast majority of common internet threats.**

If it's already effective, why are you changing it?

Quite simply, because, time moves on – particularly in cyber security. We've been running the scheme pretty much unchanged since 2014 and we believe it now needs to **evolve** to meet today's needs. And, whilst 30,000 certificates is a big figure, it's a small percentage compared to the number of organisations out there in the UK.

So, what have you been doing?

I'm glad you asked 😊

Last year we carried out an extensive consultation exercise, across a whole range of organisations and individuals in different sectors, aimed at understanding their experiences of Cyber Essentials. These included:

- government partners
- organisations that had experience of going through Cyber Essentials or Cyber Essentials Plus certification
- consumers of certificates i.e. organisations that require Cyber Essentials certification as part of their supply chain security
- organisations that deliver the scheme on behalf of the NCSC (our existing Accreditation and Certification Bodies)
- other cyber security practitioners
- and finally, organisations that were aware of Cyber Essentials but had chosen not to be certified

We were really pleased with the response to this, particularly with the positive support we got for continuing the scheme.

Generally, people liked the simplicity of a set of basic technical controls that they could implement on their systems, be tested against and, get a certificate as evidence that they had done the basics right.

Cyber Essentials evolves

The consultation also highlighted a few things that organisations found difficult and several areas where people were looking for additional or different support. Some of the common messages we took away were:

- the user journey to certification is perceived as complicated with different Accreditation Bodies operating the scheme in different ways
- organisations didn't just want certification, they wanted to know who to turn to, for help in implementing the technical controls, maintaining them and responding when things go wrong
- for those looking for confidence in their supply chain, there was confusion about the scope of Cyber Essentials assessments and about the validity of certificates
- organisations are also consuming technology differently than 5 years ago, so people were unsure of how Cyber Essentials related to things such as cloud or shared office services
- finally, there was also an appetite to explore other "levels" of confidence outside of what we know today as Cyber Essentials and Cyber Essentials Plus.

In response to the above the NCSC has established a project and have started planning for change.

A new partnership model

The first change simplifies the way we operate Cyber Essentials. Rather than having 5 Accreditation Bodies, all operating in slightly different ways and all having their own Certification Bodies, we are looking to appoint a single cyber security delivery partner to take over running the scheme.

This will allow streamlining of the end to end customer experience, as well as introducing greater consistency into how the scheme is operated and how we talk about it. This first change is key to all the others we are planning. Having a single Cyber Essentials partner will make it simpler to manage the scheme on a day to day basis. It will also streamline the development process, so we can ensure that Cyber Essentials remains relevant.

Although the new partnership model will mean one organisation operating the scheme on behalf of the NCSC, the need for Certification Bodies will continue. There will be a transition period after we have appointed the new partner, and the NCSC will work closely with them and the outgoing

Accreditation Bodies to ensure that existing certification bodies are aware of what they need to do to continue providing Cyber Essentials services. We have produced an FAQ which will introduce you to the reasoning behind the changes and processes which this process entails.

Introducing a minimum criteria for certification bodies and assessors

As well as ensuring that there is consistency in the way the scheme is operated, we want to ensure that Certification Bodies and Assessors are all working to the same standard and have a clear and consistent minimum level of Cyber Security competence.

All Certification Bodies today go through a process to ensure that they have the appropriate cyber security skills, knowledge and competence. But, how they demonstrate this differs depending on the Accreditation Body they are affiliated to. We intend to work with the new Cyber Essentials partner to define and implement a consistent minimum standard of expertise for everyone involved in implementing the scheme.

Registered certification marks

When the new partner takes over running the scheme, we will be looking to address some of the concerns about the validity and scope of certificates themselves. This will begin with the formal introduction of a one-year renewal cycle for all certificates.

Currently, although organisations are encouraged to re-certify annually, there is no automatic expiry date on certificates. For companies that are using Cyber Essentials to provide confidence in the security of their supply chain, this is not particularly helpful. Therefore, from next year, certificates will be issued with a 12-month expiry date.

Continuous collaboration and improvement

The above changes are the ones we plan to implement in the near term, but once the scheme has transitioned fully to our new partner, we intend to continue collaborating with them to introduce other changes. These include:

- **The introduction of advisory services**: consultation showed us that there is an appetite in some organisations to support themselves in improving their basic IT security, including understanding and complying with the Cyber Essentials Technical Standard. We'll work with our partner to explore how advisory services can be provided to such organisations at an affordable level

- **Measuring benefit**: whilst it's useful to know how many certificates have been issued as a measure of the take up of the Cyber Essentials scheme, it doesn't really tell us much about the ***actual*** cyber security heath of the UK. We want to try and introduce ways to tangibly measure what difference implementing Cyber Essentials is having.

- **Feedback on controls:** aligned to measuring the benefit, we also want to develop more effective feedback mechanisms to ensure that the scheme keeps pace with the technology our customers are using and new or emerging cyber threats. Chris Ensor says more about this in his blog.

- **Levels of confidence:** The current levels of the scheme are Cyber Essentials and Cyber Essentials Plus. We will be working with our new partner to establish whether there is a need for additional levels, either below the current Cyber Essentials and/or above Cyber Essentials Plus.

- **Scope of certification:** it's not always clear what systems or elements of a system have been assessed as part of the certification process. This makes it challenging for government and private sector purchasers who are relying on the use of Cyber Essentials to assess the security of their

supply chain. We will be trying to make it easier and more intuitive to understand what a certificate covers.

- **Automation:** we also want to explore innovative automated technical solutions to deliver certification services. Automation won't be the right solution for all organisations, but we believe that where appropriate, it will help make the scheme more affordable to operate at scale

What isn't changing?

We have recently carried out a review of the five technical controls and believe that none are redundant. We'll continue to monitor these and we will also look at where alternative controls could have the same effect. But, there are no plans to change the technical standard ahead of transition to the new partner.

When is this happening?

We're using the word **evolve** quite deliberately. We absolutely don't want to break something that is fundamentally working. Our aim is to improve something that's already good. So, we won't be changing everything at once.

Our priority is to appoint a new commercial partner to help us with our plans. We are currently in a commercial tendering process and expect to announce the results of this over the summer months. We'll work with our new partner to ensure that everything is in place for them to take over operation of the scheme when the existing contracts to run Cyber Essentials draw to a close, at the end of March 2020.

As we have come to expect of them, our current Accreditation Bodies are working professionally with us to provide us with all the information we need to make this transition as smooth and easy as possible. I'd like to thank them all for their help in this.

Don't panic!

One of the questions that has been raised since word of our planned changes has hit the streets is, *"Should I continue with my plans to certify, or re-certify, given the scheme is changing"* ?

The answer to this is a resounding YES! If you haven't consciously implemented Cyber Essentials, you could be vulnerable to attack now. Our Accreditation and Certification Bodies are here to help you today, so take a look at the Cyber Essentials website, and consider getting started immediately.

When will we hear more?

We have a set of FAQs on the Cyber Essentials website which should answer the majority of your questions about the transition period. The next major piece of news will be when we have completed the commercial process and have awarded a contract to the new Cyber Essentials partner. Watch this space!

Anne W

Head of Commercial Assurance Services