6 TIPS TO KICK START YOUR CYBER ESSENTIALS APPLICATION

Every business needs good cyber security

With the right protection in place your business:

1. Will be trusted
2. Will run more efficiently
3. Won't be disrupted

That means you'll win more business and can service it more quickly and reliably.

The Cyber Essentials scheme is a great way to improve the fundamental cyber security of your business.

If you don't already know about Cyber Essentials, then find out more here.

If you have done some research into Cyber Essentials already then you'll have a lot of information. Much of it, though, will be generic and theoretical. What you need next is some practical real-world advice so that you don't need to re-invent the wheel.

This guide shares the 6 most important tips I have learned, working with my clients. And that will help you reduce the time and effort it takes to kick start your application.

Tip 1 - Follow NCSC Guidance

By far the best place to start is on the National Cyber Security Centre (NCSC) website. These are the people that write the requirements for Cyber Essentials.

The key document is called the Requirement for IT Infrastructure and you can find it here.

Tip 2 - Take Time to Define Scope

Defining Scope is the foundation of your application so you need to make sure that it is done properly. Even for a small business, defining Scope can be more involved than it first appears.

I can't do it justice in a single 'tip' so think of this more as a mega-tip.

Naming the Scope

The Scope name must uniquely identify the systems to be assessed. For a small business with a simple network, this will include the entire system. The Scope can then be named after the company. Get in touch with your Certification Body or ACE Practitioner before progressing.

If parts of the system are deemed 'out of Scope' then the Scope name should reflect this and must not be named after the company.

6 TIPS TO KICK START YOUR CYBER ESSENTIALS APPLICATION

Boundaries

A fundamental boundary for a business network is the firewall [1]. If you have multiple sites, then you will have multiple firewalls. If you have a home network in Scope, then the firewall at that site must be included.

Everything inside the firewall is in Scope. In other words, any device that connects to your network – wired or wirelessly – must conform to your chosen policy.

Home Networks

Home networks are unique in that they have two separate and conflicting uses, home or domestic use for the family; and business or professional use for the organisation. Ideally you want both uses to be secure but you may find it inconvenient to impose Cyber Essentials requirements on home users. A common approach is to segregate business use using an additional firewall and a separate wireless network.

Out of Scope

If there is a component inside the firewall that you don't want in Scope, for example an old application that is no longer supported, you have three options:

- Remove the out of Scope component from the network
- Partition the component from the network
- Decommission the out of Scope component

The Cloud

Your organisation's data is likely to reside in the cloud too. You will need to include this in the Scope. The first step will be to identify where it resides and its level of sensitivity.

Most data held in the cloud will be known to you – email for example – but often, sensitive information will be shared without your knowledge. For example, almost every organisation that we work with these days has staff or sub-contractors using Dropbox without 'official' approval. You will need to approach this with a light touch if you are to discover who is using third-party data sharing applications. We'd suggest an amnesty followed by an audit.

Mobile Devices

If mobiles devices access the organisation's data, then they are in Scope. The most common use of this will be access to email. NB: This applies to any device, including privately owned devices in use by staff, sub-contractors or partners.

Acid Test

A useful way to determine what is in Scope is to ask the question, "Is there anything or anyone that can gain access, or influence the security of the data and devices in Scope?". If so, then they are in Scope and should be included.

[1] Note: A firewall may be referred to as a router, gateway or modem. Although technically these names mean very different things, nowadays they are used interchangeably – especially on smaller networks where there is only one boundary device. I will use the term 'firewall' throughout this document.

Tip 3 - Use Screen Shots

Screen shots are a very effective way to illustrate your answers.

- They save time and convey a lot of information quickly. Rather than trying to describe a firewall configuration, you can simply take a screen shot and paste it into your answer.
- They enable you to give a more complete answer which shows that you have thought through each requirement. That increases your chance of a successful application.
- It also makes it easier for the assessor to see the measures you have taken when it comes to certification. And a happy assessor makes for a smoother application.
- On a PC the Snipping Tool is a fantastic little tool for taking and editing screenshots.
- On a Mac it's a little more fiddly but if you Google "How to take a screenshot on your Mac" you'll find a really thorough article on the Apple Support site

Tip 4 - Create Policy Documentation

Creating policy documents for your business has the following benefits:

- Review and improve your cyber security processes
- Increase staff awareness

To create policy documents, you have to think carefully about how you currently approach each measure. That is a great opportunity to review and improve your processes. And once that's done, by circulating the process to your staff you increase their awareness of the issues and improve your security further.

Create These Policies:

Password Policy – This is a fundamental requirement for achieving Cyber Essentials accreditation. Go to the NCSC website from Tip 1 and look for the 'Password-based authentication' heading.

System Administration Policy – The rules for staff, third-parties and/or subcontractors that are looking after your system.

System and Data Access Policy – The rules for accessing your system and data. For example, how authorisation is given, on what type of devices, minimum security measures that should be enabled on a device. Approved locations for the storage of data.

Device and User Setup Policy – The rules that list how devices and user accounts are created and, importantly, removed from the system.

Device and User Decommission Policy – The rules that list how devices and user accounts are removed from the system.

Firewall and Wireless Policy – The rules that list how firewalls and wireless access should be configured.

Mobile Working Policy – The rules covering on what basis the system can be accessed by mobile devices such as phones and tablets.

I would also recommend that you create documents to record specific technical information, and the justification/approval process for changes to the infrastructure.

System Documentation – Key system configuration information including details of servers, networks, connectivity, IT suppliers contact details, printers, website/domain, backups and third-party applications. Avoid storing passwords here.

Firewall Approval and Configuration – A table showing a description of each change made, the justification, the approver and the date of the change. This is followed by screenshots of the firewall configuration.

Information Asset Register – A table showing the details of all data locations. This includes the type of data, what it is for, where it is stored, who has access to it, how sensitive it is, how long it should be retained for and the risks associated with it.

Important note: Remember that the information in your questionnaire answers is extremely sensitive. Make sure that the documents you create are stored securely, only accessible by authorised users and not distributed by email unless encrypted.

Tip 5 - Promote Internally to Raise Awareness

Take advantage of this opportunity to raise awareness of cyber security within your organisation.

An initial presentation to your team on the benefits of Cyber Essentials will help subsequent changes to be accepted. It will encourage staff to stick to the rules. It will ingrain cyber security into your organisation's culture.

Consider cyber security awareness training. This will empower your team to protect themselves both at home and at work.

It can also be beneficial for sales and marketing personnel to understand how cyber security can be used to help them meet their targets. By understanding the benefits, the marketing team will have a new way to promote the business; and the sales team will be able to show prospective customers that they can trust your organisation.

6. Maintain Your Cyber Security

Remember to maintain the cyber security measures you have implemented.

Cyber Essentials accreditation is one-off annual event that demonstrates you have measures in place to protect your system ***at the time of the assessment***. For those measures to continue to protect your business beyond the assessment itself they need to be maintained. That means that you need to maintain your firewall, backups, endpoint protection, system updates, user accounts, and passwords.

To achieve this, you will need to implement a series of scheduled checks on your system. Some will need to be carried out every day while others can be checked less often.

Recap

I hope that the 6 tips in this article have helped you kick start your Cyber Essentials application. You may find your head spinning with all the information. So, I thought a quick recap would help to bring it all together:

1. Follow NCSC Guidance. Read through the Requirements for IT Infrastructure document on the NCSC website.
2. Take time to define Scope. Although you may be keen to get going, taking time to get Scope clearly defined will make the process easier in the long run.
3. Use screen shots to illustrate your answers. This will save you time and increases the chance of a successful application.
4. Create policy documents to support your application. These will help improve your cyber security processes and staff awareness.
5. Promote awareness of the benefits of cyber security within your organisation. Not only will this improve the robustness of your business but it can also be used to differentiate you from competitors.
6. Ensure that the measures you've implemented are checked regularly. By doing this you will maintain a robust approach to securing your system and reduce risk.

About the Author

David Watson is an experienced and qualified technology expert. His business, Evolve Computers, has been helping small businesses keep their systems secure and stable since 2002. He is a Chartered IT Professional, a British Computer Society member and an Accredited Cyber Essentials Practitioner (Advanced). He is respected in the IT Community as a speaker and member of the CompTIA UK Executive Council.