Compliance Series

Cyber Essentials

A pocket guide

Alan Calder

itgp™

Cyber Essentials

A Pocket Guide

ALAN CALDER

IT Governance Publishing

IT Governance Publishing
IT Governance Limited
Unit 3, Clive Court
Bartholomew's Walk
Cambridgeshire Business Park
Ely
Cambridgeshire
CB7 4EA
United Kingdom

www.itgovernance.co.uk

First published in the United Kingdom in 2014
by IT Governance Publishing.

ISBN 978-1-84928-689-3

CONTENTS

INTRODUCTION

The origins of the Cyber Essentials scheme

Thousands of IT systems are compromised every day – a shocking fact. But when you consider the proliferation of cyber threats in recent years, it isn't surprising that some of them are successful. Although cyber activists and spies often get more press, most are carried out by criminals and fraudsters looking for financial gain. The most common kinds of attacks now require little skill or expertise to carry out, and use technology which is widely available online – according to the Verizon 2013 Data Breach Investigations Report, 78% of the attacks they monitor fall into this category.

The UK Government wants to be sure that partners and contractors have a basic level of security in place to protect the data stored in their systems against these low-tech cyber attacks. The Government became aware that certification to a cyber security standard was often beyond the capability of small and medium-sized organisations (SMEs) and established the Cyber Essentials scheme in response. It is based on the advice given in the earlier publications *10 Steps to Cyber Security* and *Small Businesses: What you need to know about cyber security*.

From 1 October 2014 all suppliers bidding for a range of government ICT contracts – in particular contracts requiring the handling of sensitive and personal information – must be certified to the

scheme. Furthermore, suppliers will have to be reassessed at least once a year. Organisations can be certified to either Cyber Essentials or Cyber Essentials Plus (level 2 of the scheme), which demonstrates an even greater commitment to cyber security but requires an additional investment of money and organisational effort.

Why get certified?

You are probably reading this guide because UK Government contracts can be very lucrative and your company is therefore willing to deal with a lot of frustrating red tape to get one. Cyber Essentials should not be seen as a bureaucratic hold-up to business, however. The Information Assurance for Small and Medium Enterprises Consortium (IASME), the Information Security Forum (ISF) and the British Standards Institution (BSI) have all been deeply involved in the creation of the scheme, with the result that you can meet the requirements using easy to implement, low-cost solutions.

In today's climate the business case for certification to a scheme like this goes beyond obtaining government contracts. For a start, take a look at the results of IT Governance's international 2014 Boardroom Cyber Watch Survey. We asked whether respondents had received a customer query about their company's information security credentials during the previous 12 months, and 55% of the 240 respondents said yes, a 5% increase on the previous year's survey. It is clear that cyber security is of increasing importance to private companies as well as governments.

There is also a good chance that your organisation is already compliant with many of the controls, so becoming certified is not only valuable but often quite easy.

This is no reason for complacency, however; even large organisations may not have covered every control. To ensure that your ability to bid for a contract is not undermined, to protect from future legal consequences and to make sure that you only have to go through the auditing process once, it is crucial that you ensure you are fully compliant with the entire *Assurance Framework*; this book should help you to achieve that goal.

What am I protecting?

Low-level cyber attacks are usually targeted against the most vulnerable elements of your IT infrastructure. Any hardware which can be connected to the Internet can also be compromised, including desktop computers, laptops, smartphones, tablets and servers.

Sometimes computers are hijacked so that they can be used to perform attacks on others (e.g. denial-of-service attacks), to remotely send out spam or to store illegal materials. The aim of most cyber attackers, however, is to steal data such as sensitive business information or financial records. The personal details of staff and customers are a common target, and if you have access to data that can be used for the purposes of fraud (such as cardholder data and sensitive authentication data) your organisation will be of particular interest to online criminals.

With the increase in cyber attacks on SMEs (87% were hit in 2012, up 10% from the year before according to the Department for Business, Innovation and Skills), all of the security measures required by Cyber Essentials are also general good practice which should be put in place by all such enterprises. Failure to take cyber security seriously can result in theft, fraud, damage to reputation and even legal repercussions – in other words, by putting these controls in place you are defending critical areas of your business. You are also protecting your reputation – it is highly embarrassing to publicly admit that you have been the victim of a low-tech cyber attack because it shows to all your customers that their information is not being adequately protected.

Beyond and outside Cyber Essentials

It is worth noting that the scheme only lays out the UK Government's minimum acceptable security standards, which ensure a basic level of protection against prevalent threats and reduce vulnerability to breaches. As such, the controls discussed here are just the starting point for companies which are serious about protecting themselves and their customers. Organisations facing more advanced opposition, especially targeted attacks, should create a stronger security apparatus – fortunately the security requirements laid out by Cyber Essentials are in line with well established standards such as ISO/IEC 27001 or the Information Security Forum's *Standard of Good Practice for Information Security*, and can

therefore form the central component of a more comprehensive security infrastructure in the future.

Note that due to the fact that it has been designed to cover only the most common software and hardware systems in use, certain varieties of software cannot be certified as secure under Cyber Essentials – for example, Point of Sales (POS) software, Pin Entry Devices (PED) and eCommerce applications. These systems have different vulnerabilities and therefore require some different kinds of protection on top of the basic rules outlined in the scheme.

Structure of the book

The Cyber Essentials scheme consists of three documents:

1. *Cyber Essentials Scheme: Summary* gives an overview of the entire scheme, including the scope, structure, key controls and levels of certification. It also includes a FAQ.
2. *Cyber Essentials Scheme: Requirements for basic technical protection from cyber attacks* lays out the technical requirements necessary to achieve compliance with the scheme (known as 'controls').
3. *Cyber Essentials Scheme: Assurance Framework* explains the independent assurance process for both the assessor and the company being assessed, covering both Cyber Essentials and Cyber Essentials Plus. It also discusses the scoping process.

The documents are available from the UK Government at this website: *www.gov.uk/government/publications/cyber-essentials-scheme-overview*.

This book will first examine the *Requirements* in detail: discussing the controls, explaining why they are necessary and suggesting ways to put them in place so that certification is likely at the end of the implementation process.

Secondly we will look at the *Assurance Framework*: examining the first step in becoming compliant (scoping), helping you to determine whether you are ready to undergo assessment and presenting an analysis of how the certification process works.

The final part of the book presents a selection of additional resources that are available to help you implement the controls: it includes further reading and consultancy options, and also covers some sensible steps your organisation can make if you would like to take cyber security beyond the basic level mandated in Cyber Essentials.

PART I: REQUIREMENTS FOR BASIC TECHNICAL PROTECTION FROM CYBER ATTACKS

The controls set out in the *Requirements* are relevant to organisations of all sizes, but have been chosen for Cyber Essentials because they are relatively easy to implement for SMEs and protect against a wide variety of common cyber threats. But what are the common attacks that your organisation faces, and which the UK Government are so keen to protect against?

Types of attack

The image of the hacker in popular media is usually of a lone individual in a basement, tapping away at a keyboard, trying to break into a specific computer system. This targeted attack methodology is not how most attackers operate, which is lucky because it is difficult to keep out a motivated and expert cyber criminal who is deliberately targeting your organisation.

The good news is that most cyber attackers run their criminal enterprises like a business, and it is just not economical for them to go after their targets one-by-one. Successful cyber attacks in the UK generally rely on simple technology that is widely available on the web. Such attackers employ a scattergun approach, using vectors such as spam email to go after hundreds of

organisations and individuals at once, and then opportunistically break into exposed networks – these are known as 'commodity' cyber threats. To break into a system, the attackers rely on poor technical security measures at target organisations and/or a lack of security awareness among staff – so addressing these issues goes a long way toward making your organisation secure.

The types of common attack can be split into five major categories:

1. Social engineering
   Attackers 'con' employees into allowing them to access the organisation's systems. Social engineering can be targeted – for example, the attacker might phone technical support, pretend to be a senior member of staff with a high level of access, and request that they change the password for the impersonated individual's user account so that the hackers can log in later. It is also employed in low-tech attack methods – a common tactic is to send out spam emails with virus-bearing attachments, which, when opened, log keystrokes or otherwise accumulate data (Trojans). 'Phishing' is a type of social engineering attack which many of us have encountered at some point – emails purporting to come from an authoritative source (such as a bank or credit card company) are sent out, requesting that the recipient enter their login details. The criminal can then gain access to their account to siphon off funds.
2. Denial of service (DOS)
   Attackers seek to overload a network with external communications requests to create a

server overload, preventing the target from performing its normal functions. The requests which make up the attack usually come from computers which have been infected with malware – without their owners even being aware of it. The Cyber Essentials scheme helps prevent your computer being used in such an attack.

3. Brute force
   Attackers attempt to discover a password by using a program which tries all possible combinations of letters, numbers and punctuation marks. If the target is using a weak password, such as the name of a favourite football team or a dictionary word, this process is a relatively easy way to break into a system. It is also possible for some login systems to be fooled into giving up the password – if you have chosen to let your computer 'remember' it after you have logged out, then the attacker can use this against you.
4. Physical attack
   Attackers steal data by gaining physical access to your systems. They use tactics which range from breaking into office buildings and stealing servers or laptops, to masquerading as employees to gain access during working hours so that they can install malware or infected hardware.
5. Exploiting vulnerabilities
   Attackers gain access to systems using vulnerabilities that have been discovered in applications and configurations.

Cyber Essentials provides protection against the first three types of attack, which involve the use of malware – hostile or intrusive software. It also helps you to repair vulnerabilities. Although it is not a requirement it may also be a good idea to make your office more physically secure as well – one sensible policy is to require staff to ask unfamiliar, unaccompanied visitors for identification, not just at reception but throughout the building.

The scope

The first step in becoming secure from such threats is to adequately scope which parts of your IT infrastructure need to be given a basic level of technical protection. This is defined firstly in terms of the business unit/ organisation and secondly in terms of the hardware and software used by that business unit, which will need to be made secure. The part of your IT infrastructure which stores and/or processes sensitive information will have to be included in the scope, but you can choose whether to have the rest of your organisation certified as well – this is an important decision to make up-front.

There is a helpful graphic in the *Requirements* which can be used to work out what is in scope, but the *Assurance Framework* goes into far greater detail on the subject and it is recommended that you consult that instead. This book examines scope in detail at the beginning of *Part 2*.

The five cyber security measures and implementing controls

The measures laid out in the *Requirements* have been chosen deliberately to protect against the low-tech attacks discussed above. Fully implementing these five key measures will put interlocking cyber security measures into place to defend your organisation.

The measures are:

1. Boundary firewalls and Internet gateways
2. Secure configuration
3. Access control
4. Malware protection
5. Patch management

After you have determined the scope, the next step is to implement the controls that make up each measure.

It should be noted that it is sometimes legitimately impossible to implement a control; the Cyber Essentials scheme recognises this and allows you to create compensating controls, which should be defined and put in place prior to the auditing process.

Documentation

Before you start implementing the controls, you should have established an approach to documenting your progress which can be used with all five measures. Documentation is important to ensure that the rules are being applied consistently across your organisation, and is required under the

scheme in certain cases. It will also help you to fill out the self-assessment questionnaire when trying for Cyber Essentials certification.

Your suite of documentation should be based on the controls and explicitly linked to the network and user devices which are in scope for Cyber Essentials. It should be easily accessible to every member of staff who can make changes to these devices. Rules should be put in place to ensure that whenever staff work on these devices they must consult the documentation to find out the correct way to go about the changes, and must also make a note about what they have done; this will let you know that the rules/processes of the scheme have been correctly applied.

1. Boundary firewalls and Internet gateways

A boundary firewall is located at your organisation's Internet gateways (e.g. the modem, wireless router or dedicated gateway) rather than on your desktop PC or other device, and restricts connections to and from your entire network. This is the traditional place to put a firewall, although it is now becoming more common to also have additional firewalls on the other devices that make up the IT infrastructure ('host-based' firewalls). Restricting network traffic (by allowing only connections you have authorised) makes it far more difficult for attackers using commodity threats to gain unauthorised access via the Internet. Internet proxy servers and host-based Internet protection applications can also prevent your employees from accessing websites that will pass on a virus. The

Cyber Essentials scheme therefore mandates that a boundary firewall or similar defensive apparatus must be put in place around the part of your IT infrastructure ruled to be 'in scope'.

There is a good chance that your organisation already has a firewall like this in place, especially if you are operating a small network with only one internet gateway, because most gateway devices will come with a firewall already installed. It is, however, necessary to take the following steps to make sure that it is providing the protection that it should.

Whether the firewall came installed with the product or you installed it yourself, you must ensure that the administrative password that came with the device is changed to an appropriately strong one (the default passwords may be generic or follow a specific pattern which hackers can discover and exploit). It is best to follow current guidelines about password strength.

Strong Passwords

There are a few widely accepted rules for creating a password that is difficult for an attacker to guess. A password:

- Should consist of eight or more characters and include a mix of lowercase letters, uppercase letters and numbers. Better still, include a symbol such as @, #, $ or %.
- Should not have been used recently or for another account – an online bank can probably safeguard your password, but if you have also used it for a less secure website then attackers

can steal it from there and use it to gain access to your account.

- Should not be a dictionary word.
- Should not be the same as the associated username.
- Should not include information that an attacker could find from a social media account, e.g. the name of the user's favourite football team.

Alternatively, password management software may be a solution for larger organisations.

As well as ensuring the passwords are strong, there are other ways you need to configure the firewall. Above all, you must determine what connections the firewall will allow. Restricting network traffic involves setting rules to determine which connections are legitimate and which are not – both incoming and outgoing connections, to prevent hackers from easily moving data out of your organisation. Every rule that your organisation puts in place must be approved by an authorised individual – this must be documented, along with the reason that approval was given. Any services that are not approved, and those which are vulnerable to attack because they transmit unencrypted information (e.g. Server Message Block, NetBIOS, tftp, RPC, rlogin, rsh or rexec), must be disabled at the firewall by default.

Furthermore, any firewall rules that become obsolete must be removed or disabled.

Finally, there should be no external access from the Internet to the administrative interface used to

manage the firewall configuration – if attackers can use it to disable or circumvent the boundary firewall, then they can move data into and out of your network far more easily.

If it should prove impossible to implement one or more of these controls, then alternative controls can be implemented. The *Requirements* gives the following example: if the firewall is being supported by an external services provider, then it is not practical to stop the interface from being connected to the Internet as they will have to access it remotely. Therefore strong additional security measures must be implemented (e.g. encrypting the connection, allowing only authorised individuals to access the interface, allowing only connections from whitelisted IP addresses).

2. Secure configuration

The aim in implementing this measure is to carry out a process called 'system hardening'. This consists of applying security controls which ensure that the devices and software which make up your IT infrastructure are properly configured to give maximum protection.

Correctly installing a device or a piece of software is about more than simply plugging it in. There are inherent risks in using some devices, simply because they are connected to the Internet, while other devices become a problem when they are not correctly installed or if default settings are not changed.

Default settings on computers and software can make a hacker's job easier, because unnecessary user accounts and unused applications that are left on your system are not as closely monitored. Applying the following controls will address these issues by ensuring your computers and network devices are set up for security.

All unnecessary accounts – both those created before purchase and those created for staff but no longer needed – must be removed or disabled to prevent them being misused by hackers. Your system is only as secure as the most vulnerable account, so if a default account has a weak password or is otherwise simple to break into then it is a threat to your entire IT Infrastructure – default account credentials are often freely available online or in manufacturer's documentation.

Similarly, all unnecessary software must be removed or disabled, including applications, system utilities and network services. Some software can provide hackers with access to sensitive information, while unremoved communications software (e.g. an instant messenger) could be hijacked to send data outside the company undetected.

Accounts that are in use must not be secured with a default password – and the new password should be strong, adhering to the principles laid down earlier.

The auto-run feature dictates what a system does when removable media are inserted – if it is enabled, the programs on a CD, memory stick or portable hard drive will start up automatically. Unfortunately, auto-run provides attackers with a

ITG RESOURCES

IT Governance offers three unique solutions to help you meet the requirements of the Cyber Essentials scheme at a pace and for a budget that suits you.

As a CREST-accredited certification body, IT Governance can help you to achieve certification to either Cyber Essentials (CE) or Cyber Essentials Plus (CE Plus).

Do it yourself – solution

1. You read the requirements, implement them, then complete and submit the SAQ.
2. We then review the questionnaire, conduct an external scan for CE, and an internal scan and onsite assessment for CE Plus, and issue the certificate subject to compliance*.
3. Pricing
   a. Cyber Essentials – £400
   b. Cyber Essentials Plus – £1,150

Get a little help – solution

1. We teach you what to do, give you the tools, you implement, then complete and submit the SAQ.

2. We then review the questionnaire, conduct an external scan for CE, and an internal scan and onsite assessment for CE Plus, and issue the certificate subject to compliance*.
3. Pricing
   a. Cyber Essentials – £885
   b. Cyber Essentials Plus – £1,635

Get a lot of help – solution

1. We come on site, show you what to do, and help you complete and submit the SAQ.
2. We then review the questionnaire, conduct an external scan for CE, and an internal scan and onsite assessment for CE Plus, and issue the certificate subject to compliance*.
3. Pricing
   a. Cyber Essentials – £1,245
   b. Cyber Essentials Plus – £1,995

* We will issue you with a certificate if you pass the scans and our technical assessor agrees that your questionnaire indicates compliance with the scheme requirements. The certification process is a different activity than the help and support activities we offer.

Conditions apply: The all-in fixed price solutions above are applicable to SMEs with approximately 250 staff, less than 16 IP addresses and based on one location only. Alternatively, contact us for a custom quote.

Visit *www.itgovernance.co.uk/ces-certification* for more information.

To purchase this book:

www.itgovernance.co.uk/shop/product/cyber-essentials-a-pocket-guide

www.itgovernance.eu/shop/product/cyber-essentials-a-pocket-guide

www.itgovernanceusa.com/shop/product/cyber-essentials-a-pocket-guide

www.itgovernance.asia/shop/product/cyber-essentials-a-pocket-guide

www.itgovernancegulf.com/shop/product/cyber-essentials-a-pocket-guide