Guide to Cyber Essentials - 2022

Guide to Cyber Essentials 2022

Table of Contents

Understanding the threat to your organisation

Although most organisations spend 5.6% of their overall IT budget on information and cyber security and risk management, many still don't understand cyber security. They still do not know how to keep hackers out.

Over the last ten years, we've seen exponential growth in cybercrime. According to the UK Government, 39% of UK businesses reported a cyber breach in the previous 12 months. These numbers continue to rise as we become increasingly reliant on technology within our organisations and hackers become more sophisticated. With over 65,000 cyber-attack attempts daily in the UK, the message is clear: Cyber security must be a priority for every business owner.

A significant number of organisations wish they could go back and make amends. Sadly, "It's never too late" does not usually apply to cyber security.

Who is a Threat to Your Organisation?

We often get told, during early conversations, that company x doesn't need any cyber security because no one will ever attack them. But attacks happen, and it might be an accidental error by one of your employees or a criminal attempting to gain unauthorised access to your data halfway around the world. There are five common sources of cyber threat, which are below:

Hacktivists

- Agenda or ideology.
- Examples are Anonymous, LulzSec, and the Syrian Electronic Army.

Hackers

- Status and technical challenge.
- Hackers can be good, or they can be harmful. It all depends on their actions.

State-Sponsored

- National advantage.
- Well-funded and targeted.
- Designed to gather information.

Insiders

- Privileged access to data.
- Insiders can be malicious or, more commonly, accidental.

Criminals

- Often driven by financial gain.
- Theft of data ransomware cyber-enabled or dependant

What are cybercriminals trying to do?

Cybercriminals, or criminals as they are correctly known, may have many ways to get your data:

- Criminals may infect your systems with malware to disrupt, damage, and gain unauthorised access to your computer systems.
- They may use Social Engineering techniques to manipulate your employees into divulging confidential and personal information subsequently used for fraudulent purposes.
- If your patching regime is not very good, they will exploit vulnerabilities and weaknesses in your systems to gain access to your network.
- An old but widespread attack is overloading your systems with DDoS (Denial of Service). The criminals use multiple techniques to flood and target the bandwidth and resources of your systems and then hold you to ransom. A DDoS attack uses one or more control servers that issue commands to all the compromised systems simultaneously send requests to your website or system.

Is there a solution to the cyber threat?

In 2020, 39% of UK organisations suffered a data breach or attack. We know that sounds uncomfortably high. The good news, however, is that the trend is changing. Businesses prioritise their cybersecurity programs, with 77% now saying it is a high priority for their senior management boards.

So how are these businesses responding to this cyber threat? Many companies are looking to recognise standards that will give them a baseline for good cyber security. One of the UK's most recognised standards is Cyber Essentials, and with the ever-growing push from the government, clients and suppliers, you've likely heard that name knocking around. Some organisations have gone further with monthly vulnerability scanning and quarterly or six monthly penetration testing of their internal and external networks.

Organisations around the world are seeing the benefit of aligning their security to the requirements of Cyber Essentials, and these efforts, in combination with regular security testing and sold are primarily responsible for the decline in successful breaches.

What is the Cyber Essentials Scheme?

Cyber Essentials is the UK governments cyber security assurance scheme. The Cyber Essentials and Cyber Essentials Plus scheme is run by the UK's National Cyber Security Centre and encourages organisations to adopt reasonable data security practices within their organisations. Cyber Essentials was designed by the government in 2014 primarily for small to medium-sized businesses to make it easier to protect against common cyber threats and start to put an end of the ever increasing number of small to medium-sized businesses that were getting digitally compromised by criminals.

The simplest way to think of the Cyber Essentials scheme is to think of it as a cyber security MOT for your business or organisation. You have to fulfil specific requirements to pass successfully, and your assessor will confirm whether you meet these.

For Cyber Essentials, that 'assessor' is called a Certification Body. Hedgehog Security is one of those certification bodies approved by IAMSE to deliver Cyber Essentials and Cyber Essentials Plus., as well as the maritime version of Cyber Essentials, the Maritime Cyber Baseline. They have the official qualifications needed to certify you for Cyber Essentials - that is, as long as your organisation ticks all the boxes. A large portion of the assessment is a self-assessment questionnaire, and it is these answers will determine whether you pass or fail. The questionnaire is updated annual, so if you already have your Cyber Essentials certification and you are renewing, don’t expect to be able to simply submit the answers from the previous year either.

Once you show you have all the necessary processes, policies, and controls (we have a lot of free to use templates here), you'll achieve the Cyber Essentials certification so you can demonstrate you commitment to Cyber Security to your clients, partners, and suppliers. Most importantly, you'll feel more confident that you're secure and protected.

Certification Bodies are an essential part of achieving your Cyber Essentials certificate. But what exactly are they, and how do you find one? Certification Bodies operate under the IASME Consortium, which became the sole accreditation body on the 1st of April 2020. Before, there were five accrediting bodies with varying methodologies, but the government decided to appoint only one.

IASME works with and oversees several Certification Bodies across the country, including Hedgehog Security, and each Certification Body has qualified assessors who can certify businesses and organisations for Cyber Essentials. You can visit IASME's website to see a complete overview of all the Certification Bodies.

What Are the Benefits of Cyber Essentials?

Cyber Essentials is run by the UK government and has become the standard by which the UK government holds all of its supply chains to account. You will therefore be aligning your business with the most recognised national standard.

Time, Money and Resources

With a high-level view of your cybersecurity, you can iron out any inefficiencies in your practices and maximise productivity as your team will have more time on their side.

Government Tenders

Cyber Essentials can help you get there if you pursue government tenders and contracts. Cyber Essentials is a minimum certification level requirement for any organisation looking to obtain government contracts (including the Ministry of Defence and Health), especially in the private sector.

Marketing Through Security

Obtaining Cyber Essentials can make a big difference when your organisation tries to get cyber insurance. The brokers will likely be more inclined to offer you a reduced premium as they can see your organisation is cyber safe and making every effort to protect its data.

As much as your business provides a service, you'll also utilise them yourselves - you are a client to someone. With that in mind, think how reassured you'd feel if that service was able to demonstrate to you that they care about looking after your data and keeping it secure. You'd likely appreciate their work even more than you do currently.

You want your clients to know that you take cyber security seriously. This begins with letting them know that you're making a conscious effort to protect their information. Before you know it, you'll have built a tremendous amount of trust in your client relationships and enhanced your reputation in your industry. When your clients are happy, they'll tell people about it - and who knows, those people might want to come to you for your services too.

Some organisations do not care about cyber security, and they believe it is not a priority or even a concern altogether. It's an unfortunate way of thinking and doesn't stand in this day and age.

With the Cyber Essentials certification, you can quickly demonstrate that you care about data and differentiate yourself from competitors who have yet to prioritise their cyber security. By showcasing the Cyber Essentials logos on your website and collateral, you put your organisation amongst businesses that can demonstrate they care about their data.

The UK must comply with GDPR (General Data Protection Regulation), and businesses must abide by this and the UK's own Data Protection Act. It's vital to comply with both of these for numerous reasons. Most importantly, though, your business or organisation could be liable to pay up to 4% of your turnover if breached.

If you are not Cyber Essentials Plus certified, the Information Commissioner's Office (ICO) can very quickly conclude that you did not implement enough measures to protect the data you hold. By having the Cyber Essentials Plus certification, you could be prevented the fine, as they would have been able to see you were trying to protect your data.

Cyber Essentials vs Cyber Essentials Plus

Even by achieving Cyber Essentials Basic, you're taking an essential step to show your clients and stakeholders that you are serious about your cyber security and protecting their data. However, since Cyber Essentials Plus officially verifies this, it is even more impactful. Achieving Plus demonstrates that you are going the extra mile to ensure you handle all your essential data in a secure environment.

Many government contracts, including MOD and NHS, require Cyber Essentials Plus, which is likely to pick up even more over the next few years. We recommend that you try and go to Cyber Essentials Plus to make it worth your while if you embark on your Cyber Essentials journey!

Cyber Essentials

Now that you understand how the scheme is delivered and who certifies your organisation let's look at what's involved in achieving Cyber Essentials.

Technically, there are two assessments you need to complete to be fully certified for Cyber Essentials. The 'Basic' certification must be achieved first (you must submit the assessment within three months of receiving it), and then there is the more comprehensive 'Plus' assessment. Both processes are slightly different, but you'll soon know how both work together and benefit your organisation.

Cyber Essentials' Basic' is a kind of DIY certification in a self-assessment questionnaire (SAQ) marked by an independent Certification Body. You can download the current self-assessment questionnaire direct from our website here.

How Much Does Cyber Essentials Cost?

As of January 2022, Cyber Essentials has adapted its pricing to reflect a tiered system based on organisation size.

Micro organisation	0-9 employees	£250
Small organisation	10-49 employees	£300
Medium organisation	50-249 employees	£400
Large organisation	250+ employees	£500

The Cyber Essentials Controls

What are Cyber Essentials assessing to say that it is confidently protecting your organisation from 80% of the cyber-attacks? It seeks to determine whether people, process and technology are aligned with the five critical controls. Technical controls are safeguards incorporated into computer hardware, software, or firmware. The controls for Cyber Essentials are:

Access Control: Users should only access the data they need with the correct procedure to deal with admin privileges.

Firewalls and Internet Gateways: Cyber Essentials requires that all of your devices are connected to the Internet using a firewall, both at a software level and a hardware firewall at the network perimeter.

Secure Configuration: Avoid install and manufacturers defaults and ensure correctly configured settings.

Patch Management: It is required for certification that all devices are updated every fourteen days to ensure vulnerabilities can be found and remediated.

Malware Protection: Cyber essentials check that you have the appropriate anti-virus protection for viruses, malware and other threats to your business.

Access Control

It is essential only to give users access to the resources and data necessary for their roles, and no more. All users need to have individual accounts and should not be carrying out day-to-day tasks, such as invoicing or dealing with email, whilst logged on as a user with administrator privileges, which allow significant changes to how your computer systems work.

Best Practises

- A person approves all user accounts with a leadership role in your organisation.
- You should ensure that passwords are needed to access devices and systems. Where possible, you should supplement passwords with multi-factor authentication.
- Users should not be prevented from using shared accounts.
- Stop any former employee from accessing any of your systems.
- Ensure that staff only have the privileges to do their current job.
- For administrator/root level accounts, ta formal, written-down process should be followed when deciding to give someone access. This process must include approval by a person at a senior level of the organisation. These accounts should only be used for administration purposes, and you should have a policy around this.
- You should ensure that administrator accounts cannot be used to generate internet use or access email. It is possible to achieve this through administrative controls such as a sound policy and procedure and regular staff training.
- A list or formal record of all people granted administrator accounts should exist, and this must be reviewed at regular intervals.
- Two-factor authentication must be in place for all administrative accounts, both on-premise and cloud.

Firewalls

Firewalls provide technical protection between your systems and external systems. The firewall filters anything that could harm your systems and keeps your network safe from external threats.

Best Practises

- Homeworkers should be connecting via the central office VPN.
- There should be a guest network for your client's and customers' internet access.
- Where your Managed Service Provider or IT provider wants to access systems for configuration, they should connect over the central VPN and use two-factor authentication.
- All devices must have software level firewalls enabled.

Secure Configuration

No computer will be secure straight out of the box. There is always a default administrative account, and often this is easy to find on the Internet. Default user accounts, usually unnecessary historical ones, are often enabled, and sometimes these have special access privileges. All of these can present security risks.

Best Practises

- You must remove or disable the applications, system utilities and network services not in day-to-day use.
- Remove or disable any user accounts not needed.
- Change any default passwords that may exist for all user and administrator accounts on all devices and servers to a non-guessable, strong sixteen character long password.
- Ensure every user has a non-guessable, twelve character or long password.
- You must not include predictable words in your passwords. These are words such as "password" or obvious sequences such as "12345".
- If you believe a password has become known to others, you must change passwords immediately.
- All accounts should limit the number of unsuccessful login attempts to no more than ten within five minutes. If this happens, the account should be locked for 15 minutes.
- You need to write a password policy to guide your users. It should contain guidance on choosing non-guessable passwords, not using the same password for multiple accounts, and where they can be stored.
- People outside your organisation must be prevented from accessing confidential information through external services such as VPN servers, mail servers etc.
- Auto-run and auto-play must be disabled on all of your systems.

Patch Management

You need to ensure that your software is always up-to-date with the latest patches to protect your organisation in today's world. Robust patching is a requirement of Cyber Essentials. As of the 2022 (Evendine) standard, we will check that all critical updates with a CVSS (Common Vulnerability Scoring System) score higher than 7.0 are installed within 14 days of release.

Best Practises

- Ensure all devices and applications are supported by a supplier that produces regular fixes for any security problems.
- Use licensed software by the publisher's recommendations.
- Ensure you install all high-risk or critical (7.0+ CVSS) security updates for operating systems and firmware within 14 days of publication.
- Remove older applications from your devices that the manufacturer no longer supports.

Malware Protection

Malware steals or damages information and is part of the attack chain that leads to ransomware. Malware is commonly used with attacks such as 'phishing' and social network sites to provide a focused attack on an organisation.

Best Practices

- Install a solid endpoint protection program.
- Maintain a list of approved applications for use in your environment and only permit these applications to be installed.
- Ensure auto-update is enabled for all operating systems and applications that support it.
- Automatically scan files upon access for malicious content.
- Prevent users from downloading unauthorised software.
- Block access to known malicious websites. This could be as simple as using the Quad9 project.
- Where application sandboxing is being used, ensure that applications within the sandbox cannot access data stores, sensitive peripherals and your local network.

How to Pass Cyber Essentials

The self-assessment questionnaire is split into eight categories:

1. Organisation
2. Scope of the Assessment
3. Insurance
4. Boundary firewalls and internet gateways
5. Secure configuration
6. Security update management
7. User Access Control
8. Malware protection

Sections one and two are general information and should be straight forward to pass. The rest of the sections will be either a Yes/No answer or you will need to provide an explanation. The key thing to keep in mind here is, where you need to provide an explanation, more details is better than less. Read the question carefully and then provide the evidence asked for in the question. Here is an example:

Question 7.5 asks:

> "*Do you have a formal process for giving someone access to systems at an "administrator" level and can you confirm how this is recorded?*"

We commonly have clients answer "Yes" to this and this means we have to score it as not passing and ask for more information. A good example of an answer to this question is:

> "*We have a formal process for granting system access at an administrator level. The access is requested from the head of IT and this is recorded in an email that is stored within an auditable folder of access requests. These access requests are reviewed on a quarterly basis as part of our general IT review.*"

Another example would be question 7.12 which asks:

> "*Please explain how you encourage people to use unique and strong passwords.*"

We commonly have clients answer "AD controls" or "Controlled by Office 365" but this would be a scored as a fail as the question is looking to understand how you encourage your users to use better passwords. An example answer would be:

> "*We run security awareness training on hire and then every six months. Included within this training is our messaging around the use of passphrases rather than passwords. We provide the users with links to the NCSC guidance on passwords and provide them with practical ways to create and remember passphrases along with how to monitor their own personal emails for signs of compromise.*"

As with many of the questions, it is a question of detail. The more detail the better as it means we do not have to come back to you to understand how you are achieving the intent of the question.

Cyber Essentials Plus

The Cyber Essentials Plus assessment process goes further than the self-assessment questionnaire. The Certification Body must check your infrastructure for vulnerabilities and ensure that the workstation configuration is correctly and adequately protected.

You have 90 days after your Cyber Essentials certification to achieve Cyber Essentials Plus.

What is a Cyber Essentials Plus Pre-Assessment, & Why Do You Need It?

At Hedgehog Security, we offer a Pre-Assessment option for those undertaking the Cyber Essentials Plus. The Pre-Assessment is a solution designed to assure businesses a first-time pass for Cyber Essentials Plus, involving unlimited sessions with our Chief Assessor and complete scanning to confirm alignment with the standard. The Pre-Assessment is great at highlighting which areas of your cyber security require attention and improvement and is especially useful as the Cyber Essentials requirements become more challenging.

The final Plus assessment becomes a formality if you get the all-clear with a Pre-Assessment. Still, you can sit back and relax knowing you'll pass because you've already completed all the necessary remediation, and you'll also avoid any re-certification costs!

Suppose you know your business has its sights set on Cyber Essentials Plus. In that case, you can start the Pre-Assessment simultaneously as completing your Basic SAQ, taking even more pressure off as you'll have plenty of time to complete any required remediation.

How Much Does Cyber Plus Essentials Cost?

As of January 2022, the Cyber Essentials scheme adapted its pricing to reflect a tiered system based on organisation size, meaning we have had to implement the same. The pricing is as follows:

Size of Organisation	Number of employees	Audit Only	With Assistance
Micro organisation	0-9 employees	£1,500	£5,000
Small organisation	10-49 employees	£2,000	£7,500
Medium organisation	50-249 employees	£4,000	£10,000
Large organisation	250+ employees	£8,000	£15,000

The Remote Vulnerability Assessment

We will need to have a list of all your external facing IP addresses and subject all of these to a vulnerability assessment. For the vulnerability assessment, we are looking to:

- Identify all the IP addresses currently in use. This includes and Infrastructure as a Service cloud systems.
- Vulnerability scan all the IP addresses on all 65,535 TCP and UDP ports.
- Confirm that there are no vulnerabilities with a CVSS v3 score of 7.0 or higher.
- Confirm that no default passwords are in use.
- Confirm that defences are in place to prevent password guessing and credential stuffing attacks.

For the remote vulnerability assessment, we will be using one of our remote scanners, hosted within our datacentre.

Best Practices

Perform a vulnerability scan your externally facing infrastructure yourself, or through a third party every month and

- address all vulnerabilities with a High or Critical rating immediately.
- address all Medium rating vulnerabilities that are exploitable within the month.

Authenticated Vulnerability Scan

The authenticated vulnerability scan is performed against a sample set of end user devices, services, and IaaS (Infrastructure as a Service) instances. This is performed to identify missing patches and security updated that leave vulnerabilities present on the system that threats could easily exploit.

The assessor will use the output of scan to identify vulnerabilities that meet any of the three following criteria:

- The vulnerability is described as High or Critical risk by the vendor
- The vulnerability has a CVSS v3 score of 7.0 or higher
- There are no details of the level of vulnerabilities the update fixes provided by the vendor.

If there are nay vulnerability that meet the above, and for which the vendor provided patch has been available for more than 14 days prior to testing, the assessor will issue a failure for the Cyber Essentials Plus assessment.

Virtual patching is not an acceptable mitigation to the security vulnerabilities of legacy unsupported operating systems long term and will not be recognised as a mechanism for compliance and so a Pass cannot be issued is virtual patching is used.

We have a document available online that details how to run these yourself should you wish to do it prior to the audit. The credentialed scan guide document is available here.

The auditor is looking to confirm that there are no High Risk or Critical Risk vulnerabilities present on the systems and that there are no vulnerabilities with a CVSS version 3 Score higher than or equal to 7.0.

Best Practises

Perform an authenticated vulnerability scan of your internal networks every quarter and

- address all vulnerabilities with a High or Critical rating immediately.
- address all Medium rating vulnerabilities that are exploitable within the month.
- Identify any areas for improvement and put an improvement and patching plan together for the coming quarter.
- Scan for localised sensitive information, such as bank details stored on workstations or in areas where they should not have been stored.

Workstation Review

Your assessor will conduct a workstation review, which is a technical assessment of a sample set of your systems in use within your organisation. This involves the assessor connecting to each of the systems in the sample set for the technical review. The assessor will be looking for proof that:

- All workstations are fully patched and up to date within the last 14 days
- That auto-update is enabled
- That the endpoint protection software is up to date and malware/AV signatures were updated in the last 24 hours
- That there is no unnecessary software installed

The assessor will then send a series of NCSC approved test malware files to the user's email and will observe the user receiving the email and attempting to open the files. None of the attachments should be successfully executed.

The assessor will then send the user a link to a portal to download the series of NCSC approved test malware files. The assessor will observe the user attempting to download and execute these files. Again, as with the emails, none of the files should execute.

Multi-factor Authentication Configuration

This is a new test for 2022 and the purpose is to test cloud services declared in the scope to see if they have been correctly configured for multi factor authentication (MFA).

To assess this, your assessor will:

- Observe users accessing cloud services using their organisation issues accounts on an untrusted device or from an incognito or privacy-mode browser session.
- If the above is not possible, the assessor will share an incognito browser session from the assessor's workstation and then observe the use accessing the cloud service.
- These are repeated for each authentication service in use.

Testing Account Separation

This test is performed on any of the sample set of end user devices, servers, and cloud environments where administrative processes can be run. When logged in with a standard user account, the assessor will observe a user attempting to run an administration process for the sampled operating systems with the current logged in account.

The Cyber Essentials Process at Hedgehog Security

Get in touch

Give us a call or email to let us know more about your business so we can best advise you on our Cyber Essentials service options. We will need to know how many employees you have at your organisation to provide you with an accurate quote.

Achieve Cyber Essentials

We will grant you access to IASME's portal and guide you through getting your business certified for Cyber Essentials via email or 1-2-1 teams or zoom sessions with an assessor, depending on the level of support you require. The Basic SAQ and review can often take less than 24 hours but don't forget it must be completed within six months of you gaining access to the portal. You will get your logos, certificate, and report within 4 hours of achieving certification.

Cyber Essentials Plus Pre-Assessment

Many businesses fail the Cyber Essentials Plus assessment on their first attempt. We try to ensure you pass Cyber Essentials Plus the first time, and we do this by highlighting any existing issues so your IT provider can fix them before the actual Cyber Essentials Plus assessment. We will spend time with you on 1-2-1 sessions via teams or zoom to go through everything that is needed to achieve Cyber Essentials Plus and will help you get the right level of controls in place to ensure success.

Achieve Cyber Essentials Plus

We will carry out your final Cyber Essentials Plus assessment, and once you have officially passed, you'll get your logos, certificate, and report.