Key Controls of Cyber Essentials

urban.

The 5 Key Controls of Cyber Essentials.

Introduction

Cyber Essentials - An Introduction

The modern world of work is full of cyber security vulnerabilities, so it is essential that you do everything in your power to ensure the prolonged security of your systems, systems that contain your clients' sensitive data. That is where Cyber Essentials comes in.

Cyber Essentials is a government-backed scheme designed to assist businesses in protecting themselves from online threats. Since the scheme was released on the 5th June 2014, over 30,000 businesses countrywide have achieved the highly coveted accreditation.

The Cyber Essentials accreditation can be split into five categories, all of which must be implemented and maintained to a certain high standard. They are as follows:

- *Firewalls*
- *Secure Configuration*
- *Anti-Malware measures*
- *Applying Access Controls*
- *System maintenance.*

Sounds like a lot of effort, doesn't it?
I agree, so why would you go to all the effort of getting a certification in the first place?

Why bother with Cyber Essentials?

Once the measures are in place to achieve the Cyber Essentials accreditation, it is estimated that you are protected against roughly 80% of threats – not a number to frown about at all.

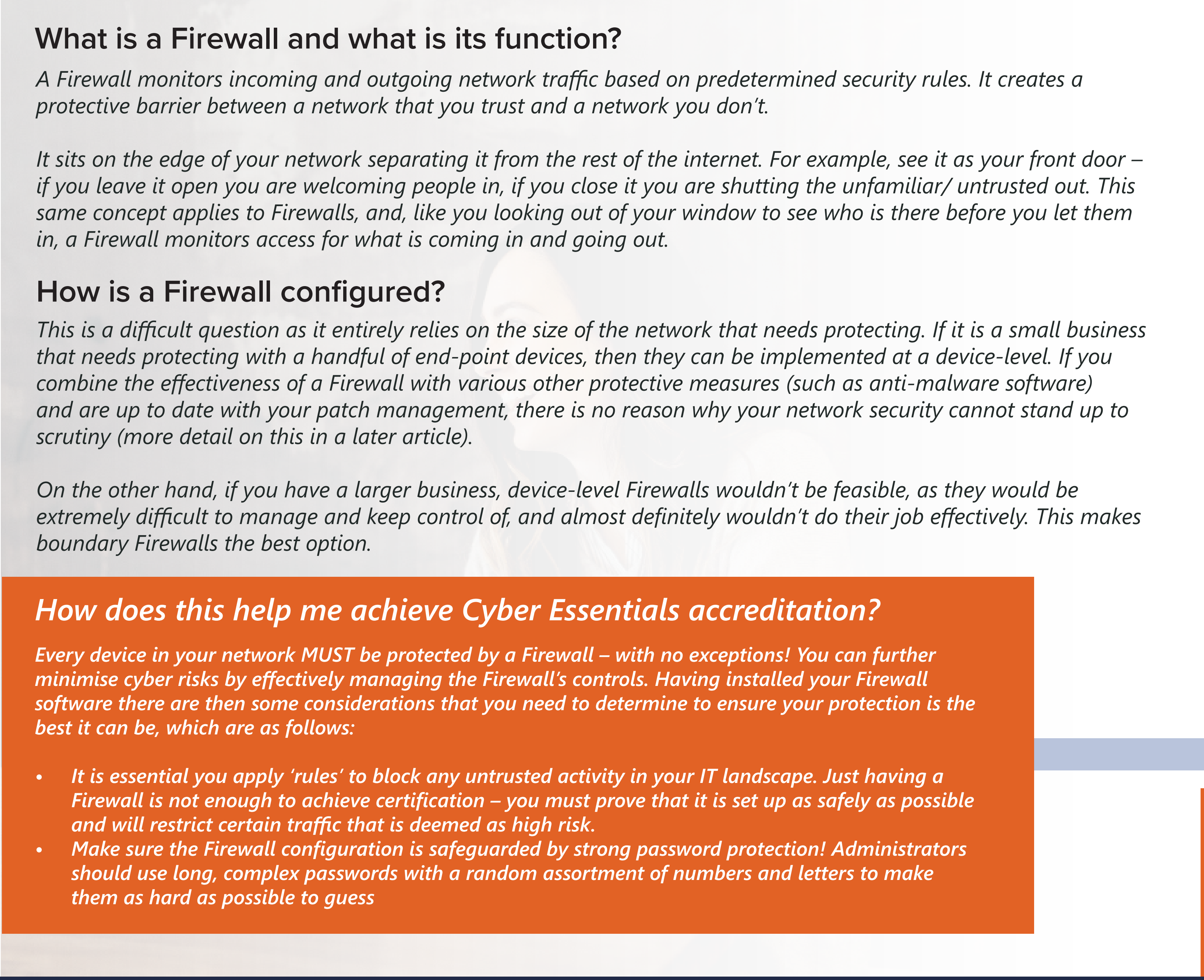
The Cyber Essentials accreditation is also very well received by a lot of businesses, and, Government departments require you to have it just to bid for their contracts! Depending on the sensitivity of the data being handled, they may want you to have the slightly superior Cyber Essentials Plus package.

Cyber Essentials will also help you satisfy the security principles of GDPR and reassure you that you are compliant to the regulations, in turn making it a good investment not just for now but also into the future. It also evokes a lot of trust from customers – having an accreditation to show that you can not only talk the talk when it comes to cyber security but also walk the walk will also likely have great reputational benefits for the organisation.

CYBER ESSENTIALS CERTIFIED

CYBER ESSENTIALS CERTIFIED PLUS

Firewalls



What is a Firewall and what is its function?

A Firewall monitors incoming and outgoing network traffic based on predetermined security rules. It creates a protective barrier between a network that you trust and a network you don't.

It sits on the edge of your network separating it from the rest of the internet. For example, see it as your front door – if you leave it open you are welcoming people in, if you close it you are shutting the unfamiliar/ untrusted out. This same concept applies to Firewalls, and, like you looking out of your window to see who is there before you let them in, a Firewall monitors access for what is coming in and going out.

How is a Firewall configured?

This is a difficult question as it entirely relies on the size of the network that needs protecting. If it is a small business that needs protecting with a handful of end-point devices, then they can be implemented at a device-level. If you combine the effectiveness of a Firewall with various other protective measures (such as anti-malware software) and are up to date with your patch management, there is no reason why your network security cannot stand up to scrutiny (more detail on this in a later article).

On the other hand, if you have a larger business, device-level Firewalls wouldn't be feasible, as they would be extremely difficult to manage and keep control of, and almost definitely wouldn't do their job effectively. This makes boundary Firewalls the best option.

How does this help me achieve Cyber Essentials accreditation?

Every device in your network MUST be protected by a Firewall – with no exceptions! You can further minimise cyber risks by effectively managing the Firewall's controls. Having installed your Firewall software there are then some considerations that you need to determine to ensure your protection is the best it can be, which are as follows:

- ***It is essential you apply 'rules' to block any untrusted activity in your IT landscape. Just having a Firewall is not enough to achieve certification – you must prove that it is set up as safely as possible and will restrict certain traffic that is deemed as high risk.***
- ***Make sure the Firewall configuration is safeguarded by strong password protection! Administrators should use long, complex passwords with a random assortment of numbers and letters to make them as hard as possible to guess***

Secure Configuration

Default security settings

'I already have default security settings on – that will do, won't it?' I hear you say, and the simple answer is NO, under no circumstances are the default security settings enough. Factory/ Default settings are relatively insecure due to them being designed to be as unrestrictive as possible to enable fluidity for the customers when having just purchased the system – it also allows them to set their own settings from a blank canvas. To stand a chance of achieving Cyber Essentials accreditation you will have to adopt much better levels of security than just those default settings.

The modern workplace is very hectic, so it can be hard to find time to do anything apart from the normal essential work functions. This being said, it is essential that, as services fall in and out of use and you acquire new hardware, you stay proactive and ready to make them and your systems as safe and protected as you can. Cyber criminals target poorly configured systems intentionally so, as a business owner, you need to be as vigilant as possible – you must find time to stay proactive.

Ways to configure your system securely:

1. Carry out vulnerability scans
It is a good idea to have a schedule for regular vulnerability scans with the intention of flagging potential security concerns. This won't stop things from sneaking in under the radar but will allow you to work out a course of action to rectify any issue the scan uncovers.

2. Establish a software update policy
Policies are important, mostly because they force you and your team to stand up and take action. You, as the manager, will lead by example and your team will follow them under the threat of the ramifications if they don't. Draw up policies relating to the installation of important, business-critical updates. A schedule with clear guidelines for how often updates are needed for a particular application or programme is essential to ensure any issues are fixed as promptly as possible.

3. Only use supported software
By using unsupported (Legacy) software you are leaving your entire network vulnerable. Unsupported software is that which is no longer updated and patched by the vendor – most software continues to work once support stops so some don't even realise the software is unsupported, but just because it still runs it doesn't mean it's safe. When there is no team dedicated to creating and launching updates to guarantee its safety this leaves security loopholes for cyber criminals to exploit.

Malware Protection

What is it?

"Malware? What's that?", I hear you say. You wouldn't be blamed for not having heard of it as it is rarely referred to by its technical name – but have you heard the term 'virus'? Malware is one of the world's most common forms of virus – it is defined as any software that is designed with the intention of causing damage to a server, computer, client, or network.

How does it work?

Malware is tricky. It uses many different methods to gain access to your system and comes in many different forms. One of your users could have – inadvertently – browsed a compromised website, they may have opened a file from a removeable storage media, or (most likely) it comes down to something as simple as opening an email that, unfortunately for the user, is infected and allows the Malware to take control of the entire system. If the Malware is successful, it has the power to cause business-defining damage to your entire system.

The fight against Malware:

Understandably, you are concerned – Malware could reap untold havoc on your entire system. But but don't worry – there are measures you can take to give your systems the best possible chance of fending off an attack.

Approved purchases

Only download apps for devices that are from the manufacturer approved shops. Apps from unknown or unreputable vendors may not have been checked for Malware before your purchase.

Your staff must be warned of this; under no circumstances should they purchase tools from unreputable vendors. Apps from widely known manufacturers are supported and are safe to use (some examples of these include Google Play store and the Apple App Store); these are safe because they have dedicated teams monitoring them to ensure that they are as secure as possible – making them very difficult to penetrate by Malware.

Malware Protection

Anit - Virus Software

You must have anti-Virus software implemented on all computers and devices both at home and in the office. Yes, most of the popular brands of operating system come with a free type of anti-virus software as standard, but this is NEVER good enough to protect your systems – especially not on a business level.

These tools are typically very basic and offer limited protection against the sophisticated threats you are likely to face in your business. Smartphones and tablets require a completely different method – these methods are easily found online; just search the name of your device followed by 'end-user security guidance' and follow the instructions, which should put you in good stead.

Sandbox

No, we haven't lost our minds – we aren't referring to a Sandbox in a playground but to a Sandbox security mechanism that separates programmes from other parts of the network – in the process stopping them from being harmed.

The Cyber Essentials accreditation requires that you implement one of the bullet points above in order to ensure your devices are as protected as possible from Malware, whilst simultaneously gaining you the certification.

What are the consequences of a Malware attack?

As we are sure you already know, viruses are never a good thing for your computer – and Malware is no different. It can cause many different problems – depending on its sophistication and how far it has managed to intertwine itself into your vital systems.

Most attacks are financially motivated. Ransomware attacks, for example, (one of the most common forms Malware takes) have risen in popularity due to the sheer number of successful attacks and the ease of carrying out such an attack. According to Cognyte, "Ransomware attacks nearly doubled in the first half of 2021; 1,097 organizations were hit by ransomware attacks in the first half of 2021. In contrast, our(their) 2020 report found 1,112 ransomware attacks for the entire year. These attacks involved data exfiltration and the leakage of victim's data." [1] You could be next!

[1] https://www.cognyte.com/blog/ransomware_2021/

Access Controls

The Aim of Access Controls

The objective of implementing access controls is to ensure that only the people required to have access to applications, networks, and computers actually have it; if their role doesn't require access then there is no need for them to have it. Cyber Essentials want user accounts to be assigned to authorised individuals that need access, not just to anyone.

The current climate has dramatically increased the need for efficient access controls. They should have been at the very top of your business security concerns anyway but, with the world of work gradually converting to an at least partially remote one, what was once a need is now a priority.

The risk of information being lost or stolen can be reduced dramatically if you only allow access to authorised personnel with user accounts that mirror their station in the business. User accounts in your business allow the use of applications, devices, and access to sensitive information – information that, if released or stolen, could cause serious financial and reputational ramifications for you, your team, and your organisation as whole.

The consequences of 'special' access privilege accounts – those that allow access to devices, applications, and information – being compromised could be disastrous and potentially incapacitate your entire organisation. In some circumstances they could even be used as the vessel for an attack on a larger scale – if your reputation, team, and bottom line weren't affected by the original attack then they will be after the second one!

Let's take administrative accounts for example – they typically allow the use of software that has the power – if in the wrong hands – to render your security measures useless. Every company has an administrator that will have access to these accounts – this is why making a revised decision on who has access to each account should be an immediate priority.
In order to apply for Cyber Essentials you must have control over the user accounts and the privileges granted to each and every one. You need to have a user account creation and approval process in place within your organisation, and to authenticate users before granting them access to apps and devices – obviously, whilst ensuring you use unique credentials for each.

Be sure to disable or remove user accounts when they are no longer needed, remove or disable any access privileges that exist to an individual's account when they are moving to a department that doesn't require it, and implement two-factor authentication using only user administrative accounts that need access to complete any administration duties.

Patch Management

In the remainder of this document we will explore Patch Management – the last of the five controls that will get you on your way to a cyber secure future.

You must keep your software and devices up to date – that is very important. Bearing mind the rate at which cyber attack sophistication is advancing, it is essential that you have all your devices equipped with the very latest protection – or else you run the risk of leaving your entire technological landscape open to problems and – depending on their severity – they could be business incapacitating ones. You can't just assume that because you have taken your devices home from the office that they are safe – it doesn't matter where they are physically situated; if they are vulnerable, then they are vulnerable!

We all see updates on our phones and laptops as a bit of a nuisance, and that is understandable – they usually take a while to download and install and seem to appear at the most inconvenient of times. Nonetheless, we accept them because they make our experience using the device or programme better. This is usually done by adding new features and improving functionality, but what most don't realise is that it is their job to patch any security vulnerabilities that have been discovered since the last update.

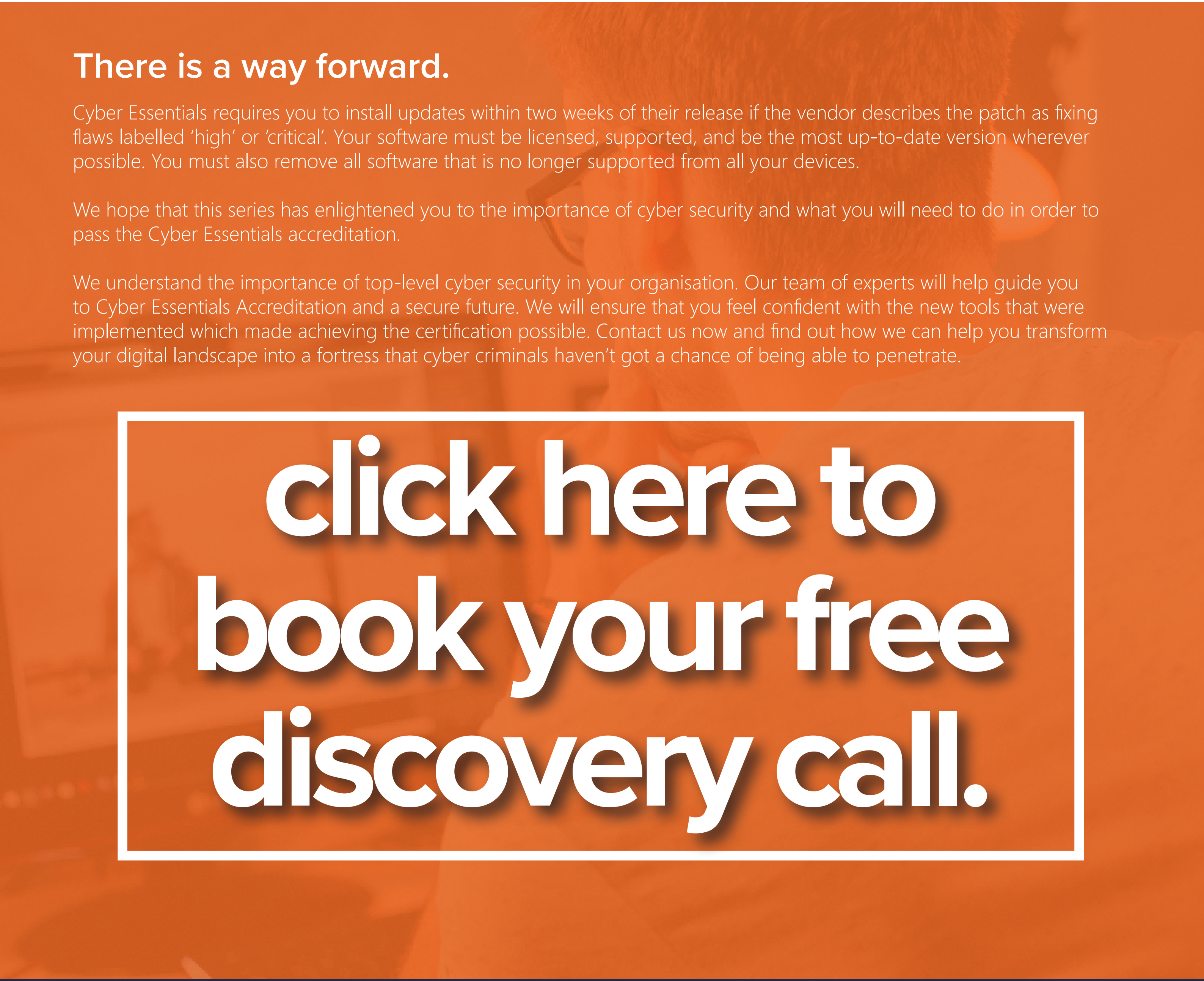
A manufacturer will make it their prime concern to remedy any security vulnerabilities at the soonest instance – it is, after all, beneficial for them to do so, because, if you were using their device and it wasn't secure, it could result in a security breach. Having suffered from one you are unlikely to use that device, software, or even manufacturer again. *Make updates automatic wherever possible!*

The evolution of tech.

All IT has a lifespan. Technology is constantly evolving, with new tools and features being released everyday, with more weird and wonderful uses and capabilities. With these developments happening so rapidly it does quickly make older – previously integral – tech surplus to requirements.

These advancements in technology are mirrored in the Malware designed to attack it. With this in mind it is essential that updates are regular – yes, this can be inconvenient, but with the evolution of technology only increasing in momentum there isn't much of more importance in the quest for cyber security. If a device or software ceases to be supported by the provider it is imperative that you start looking for, and purchase, a modern, equipped replacement as soon as possible – delaying could have serious consequences.

We can make it happen.



There is a way forward.

Cyber Essentials requires you to install updates within two weeks of their release if the vendor describes the patch as fixing flaws labelled 'high' or 'critical'. Your software must be licensed, supported, and be the most up-to-date version wherever possible. You must also remove all software that is no longer supported from all your devices.

We hope that this series has enlightened you to the importance of cyber security and what you will need to do in order to pass the Cyber Essentials accreditation.

We understand the importance of top-level cyber security in your organisation. Our team of experts will help guide you to Cyber Essentials Accreditation and a secure future. We will ensure that you feel confident with the new tools that were implemented which made achieving the certification possible. Contact us now and find out how we can help you transform your digital landscape into a fortress that cyber criminals haven't got a chance of being able to penetrate.

click here to book your free discovery call.

urban.

Coppergate House, 10 White's Row
London, E1 7NF

020 7749 6899 | urbannetwork.co.uk