Cyber Security Checklist.

vostron

Educating your business

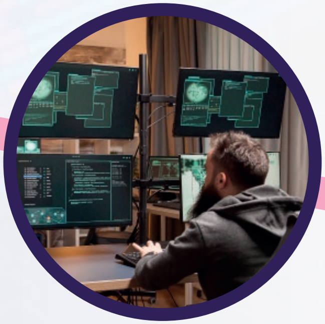
on cyber threats.

The Threats...

Everyone in the civilised world has internet connected devices intertwined into their lives, both in the workplace and otherwise, so it comes as no surprise to learn that the criminal community has seen an opportunity and are taking advantage of it. Criminals are opportunistic. Why would they go out and commit crime when they can do it from their own front rooms? We don't have to simply accept our fates though, there are actions we can take to be sure that our systems are as protected as they can be. Predominantly, the main reason that people are becoming victims of cyber attacks is a lack of knowledge regarding the subject; this article will hopefully change that by enlightening you and therefore better prepare you going forward.

So, what are some of the methods that cyber criminals use to attack your systems?

Ransomware



Phishing

Malware

...and what they are.

Ransomware

Ransomware encrypts the data on your system and denies you access to it – this can make it one of the most frustrating forms of attack of them all.

The cyber criminal will take over control of your data and demand a ransom for its safe return. Cyber criminals will force you into paying the ransom quickly by setting tight time restrictions on when it needs to be paid by. They do this under threat of deletion – or even worse – distribution of your sensitive data.

Phishing

Phishing is a form of cyber attack that takes place via email. The attacker sends email that is cleverly masked as though it is sent from a trusted source, be that a person within a business that you regularly engage with, or perhaps a brand or government department that would carry an equal level of recognition and trust from most people.

The emails themselves create a problem, which could take the form of an invoice or fine to pay, or a requirement to reset or update credentials or personal information – a problem that within its nature forces you to act with a sense of urgency, and with that urgency, act rashly and therefore fail to fully vet the legitimacy of the email and fall victim to the cyber attacker.

Malware

Malware can be particularly devastating. Its main aim is to steal your data but is designed with the intention of causing damage, destruction, and chaos on your system. Malware is unique in the fact that it is often designed, orchestrated, and managed by a group of cyber criminals rather than just one person. The group will sell the software on the Dark Web for others to use or use it themselves.

The list of potential ways that your systems could be under attack is endless, but with knowledge on these – the most common of attacks – you and your team can begin to implement ways to protect your organisation from what could be a business debilitating attack

Directly Protecting Yourself.

Documented Policies

Documented policies are very important. Having policies that are clear to understand and are known and signed by all makes your organisation more secure from the get-go. The policies must outline the security guidelines and obligations of employees when using the company systems or networks.

The policies enable you to be certain that your employees observe adequate security measures and procedures at all times – with a signature next to it to be sure that they have read and understood what is expected of them, and if they don't there will be consequences. You can outline this in the policy.

Acceptable use Policy

A cyber security checklist should include an acceptable use policy. An acceptable use policy will consist of rules regarding the use of your organisation's assets or data. Having this in place will ensure that your team are only using the tools at their disposal as instructed and not in such a way that could jeopardise the cyber security of your business.

You should make all new employees – and anyone with access and use of the system – read and sign this policy. By signing your users are agreeing to use the information at their disposal and the systems they reside on as securely as possible.

Modern and up to date software tools

Every business should use modern software and tools wherever possible. Using up-to-date software is vital to ensuring your business is secure. Modern software and tools are developed with the latest cyber security dangers in mind, whereas using legacy operating or software systems can inadvertently be making your business a target.

Don't jump to conclusions – modern up to date software doesn't necessarily mean that it is entirely secure (there are always vulnerabilities and new ones being developed every day) – this is why it is essential that you have a patch management programme too. Take advantage of patches released by vendors because they will not only improve the software, app, or programme but also bolster its security capabilities too.

Methods of Prevention.

Employee Education

You must include employee training in your cyber security checklist. The right training will provide employees with the skills to securely navigate your systems using the data and the system as they see fit. Taking it one step further, your team will be more likely to find, assess, and report a security issue if they happen to come across one.

This education should include lessons on how to; secure their emails, cloud accounts, personal devices (should they be being used for business), and information systems. Education around Phishing emails in particular is important – they need to know how to identify one and the actions they should take once having received and identified it.

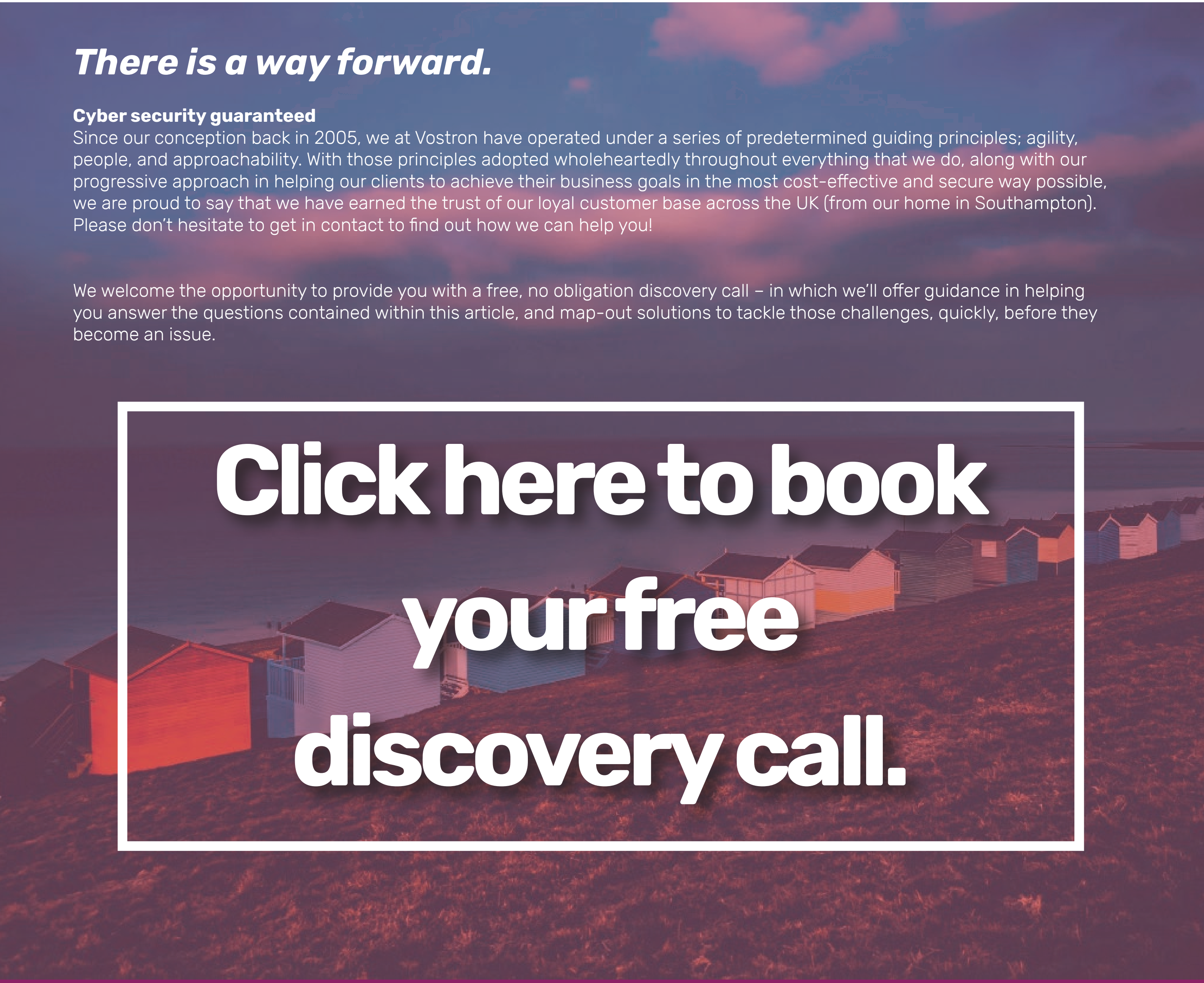
An effective data backup policy

As you know, just because you have the most powerful security solutions and procedures in place, there is no guarantee that you will not be a victim of a cyber attack. So, it is best to be prepared for the worst-case scenario too. Businesses need to outline and enforce an effective disaster recovery policy. In the disaster recovery plan different parts of your business will have a different set of actions to take in the event of an attack – developing these 'personal' disaster recovery policies will put you in good stead to containing the attack.

By continuously updating and improving your disaster recovery policy you employees will know their roles to complete in order to ensure a speedy recovery of critical data, networks, or computer systems.

Sticking to this checklist will allow you to feel slightly better about the security of the technological landscape in your workplace!

Securing your business.



There is a way forward.

Cyber security guaranteed
Since our conception back in 2005, we at Vostron have operated under a series of predetermined guiding principles; agility, people, and approachability. With those principles adopted wholeheartedly throughout everything that we do, along with our progressive approach in helping our clients to achieve their business goals in the most cost-effective and secure way possible, we are proud to say that we have earned the trust of our loyal customer base across the UK (from our home in Southampton). Please don't hesitate to get in contact to find out how we can help you!

We welcome the opportunity to provide you with a free, no obligation discovery call – in which we'll offer guidance in helping you answer the questions contained within this article, and map-out solutions to tackle those challenges, quickly, before they become an issue.

Click here to book your free discovery call.

vostron

The Arch Building, Southampton
Hampshire SO18 3HW
02380 111 111 | vostron.com