The battle against cyber crime. And how to win.

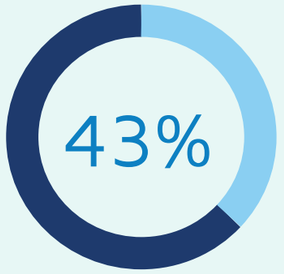
Helping organisations understand the risks of a cyber attack, how to reduce that risk and automate against new risks.

01 The fast-changing risk landscape

In today's era of digitalisation and cyber crime, organisations are increasingly worried about how to defend themselves against data breaches, cyber attacks and insider threats. Research shows that 74%* of UK businesses consider cyber security to be a high priority.

They are right to be concerned. As new devices, technologies and apps are introduced every day, different types of risk are threatening businesses. Automated **cyber attacks** are adding a new dimension of risk and rendering manual security systems obsolete.

In this rapidly evolving risk landscape, it's critically important for organisations to stay well-protected. Yet many, while recognising the dangers, are unsure of the best action to take and do not have a formal **cyber security** policy in place.



of UK businesses experienced a **cyber breach** in the last 12 months but **only 27%** have a formal cyber security policy*

*Cyber Security Breaches Survey 2019, Dept for Digital, Culture, Media & Sport

Your easy read guide to cyber security risk

This Charterhouse e-guide takes you through the key aspects of **cyber security** risk. Find out where security attacks come from, how to minimise your risk and combat new threats using automation. And learn how to quickly evaluate your business risk with a **FREE Cyber Security Review.**

02 The business risk?

Reputation: the biggest loser

Businesses often pay a heavy price for being under-prepared for **cyber breaches**, but many underestimate the full impact, which often includes financial cost, operational disruption and reputational damage.

Typically, the most serious side-effect is a loss of reputation, when a breakdown in systems, services or product quality triggers a collapse of trust and confidence. A tarnished public image can easily result in a decline in customer demand, income and share value. Rebuilding credibility might take months or years and, in the worst cases, the fallout could be irreparable.

Successful cyber attack

When an organisation is, unfortunately, on the receiving end of a successful cyber attack, one of the biggest immediate impacts is on the operational elements of a business. The business very quickly needs to shut down their network, meaning a change in the way communications are handled both internally and externally, loss of production or billable hours for example in the manufacturing or service industry.

Understanding the operational risk to the business can support the organisation making the right investments and process changes, to improve your security posture and reduce the risk.

Cyber attack puts the brakes on Kwik-Fit's reputation

When Kwik-Fit suffered a malware attack in January 2019, staff were unable to track appointments, book vehicle repairs or manage customer requests. Customers vented their frustrations on social media, the story was run by news channels and (unfounded) fears spread that customers' personal data had been compromised. Kwik-Fit's reputation was suddenly in doubt and the company had to work hard to regain public confidence.

02 The business risk: Where do security threats come from?

Here are five of the most common factors that increase your vulnerability to attack:

Unreliable people.

Of course criminals are an obvious source of threat, as are disgruntled employees who might decide to enact revenge by deliberately breaching your defences. But the behaviours of innocent employees can also pose a serious risk. If they operate hardware or software for work purposes which are not approved or supported by your IT department, these shadow IT activities fall outside the protection of your corporate security systems. A simple action such as an employee storing business data in a personal Dropbox account could introduce significant security risk.

Lack of visibility.

A lack of understanding about sources of threat and where vulnerabilities are puts your business at greater risk. This visibility of risk becomes even more blurred as employees operate personal devices and applications for work-related tasks.

Under-investment.

Many organisations fail to grasp the importance of having a clear **cyber security** policy and investing sufficiently in high-quality security systems. Without access to the right technologies and expertise, your business could pay a heavy price in the long run.

Slow response.

Failure to identify and remedy a breach quickly makes the consequences of attack go from bad to worse. Timely response is critical, especially in the case of automated **cyber attacks,** which are especially difficult to defend against.

Too much choice.

The market offers a bewildering choice of security solutions from hundreds of vendors and resellers. So, it is hardly surprising that some businesses are overwhelmed and end up investing in a security system that doesn't quite meet their needs. Any lack of specification or future-proofing can lead to unseen security gaps and vulnerabilities.

03 A world of threats: are you prepared?

Stay one step ahead of the **cyber criminals** by asking these key questions:

How confident are you that your various security solutions would protect you from a zero-day attack?

Every organisation should use next-generation technology and not rely on legacy systems, such as antivirus or port and protocol firewalls. Deploying a correct next-generation solution ensures your systems are automatically re-programming themselves as and when new threats are identified in the world, and reduces the probability of a zero-day attack.

When did you last complete a best-practice assessment on your firewall?

Organisations often install a firewall and only make changes to it when something isn't working. How often are you checking for misconfiguration? You should be running regular best-practice assessments on your firewall to identify issues and ensure your security position is keeping up with the increased threat.

What are you doing to stop the use of shadow IT?

Shadow IT is an increasing concern for organisations, especially since GDPR has thrown a sharper focus on the issue of data loss. Easy and effective reporting on the use of SaaS applications allows your organisation to decide what is sanctioned, tolerated and unsanctioned, and apply granular user and app-level control to protect your data.

03 A world of threats: are you prepared?

Stay one step ahead of the **cyber criminals** by asking these key questions:

Are your security products talking to each other or creating noise which is difficult to manage?

Many organisations are using siloed tools, which naturally create security gaps. No matter where your data is (cloud, endpoint or network), each location needs to be instantly aware of any threats, otherwise some of your data remains vulnerable to attack.

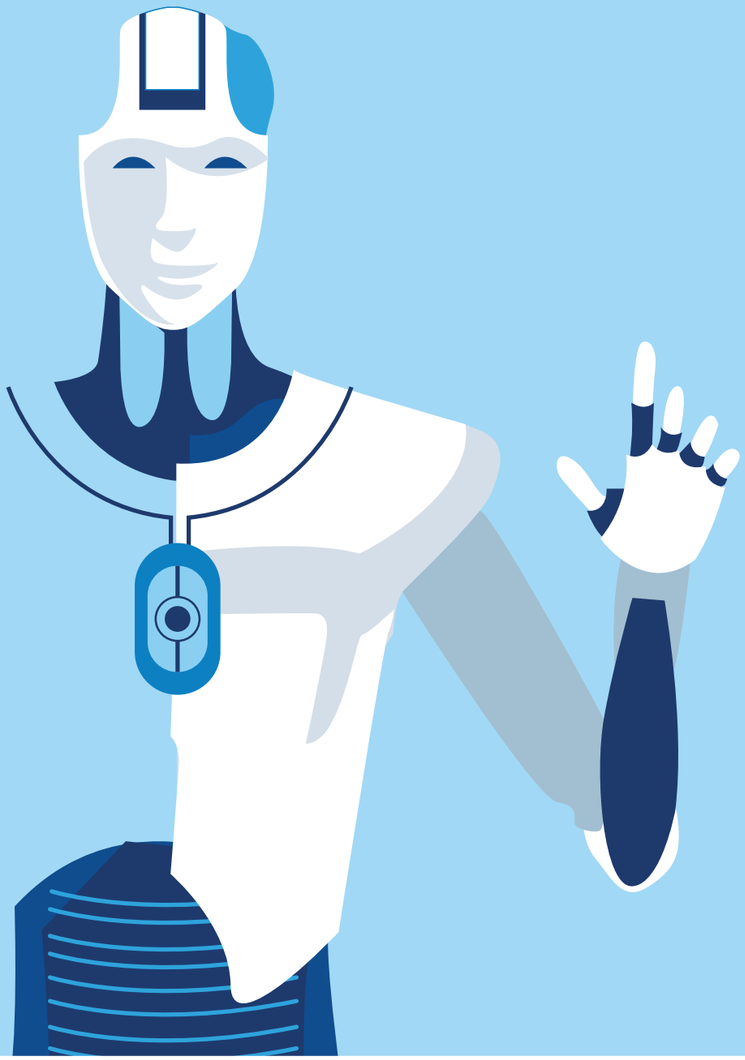
Are you relying on humans to protect you from machine automated attacks?

As attack automation becomes the new norm, using humans to try and keep up with the huge volume of attacks reduces your security posture and increases your vulnerability. Automating your defence is the only way to ensure your security posture doesn't suffer. Now is the time for machines to fight machines.

How quickly can you identify a successful attack?

Most organisations struggle to identify a successful attack within weeks, let alone as it happens. By then, it is already too late and time to implement your cyber security response plan and ICO notifications. Organisations need to be able to identify an attack in real time and stop it before a data breach occurs. This is best achieved using behavioural analytics and machine learning.

03 A world of threats: are you prepared?



Stay one step ahead of the **cyber criminals** by asking these key questions:

What visibility do you have of current vulnerabilities on your network?

Although many businesses pen-test annually, most do not check for vulnerabilities during the intervening 364 days. This means you could have a vulnerability sitting on your network for almost a year before it is identified. Implementing a solution that gives you visibility on a more frequent basis enables you to protect your organisation from a successful exploit.

Assess your security risks

The first step to maximising your protection is to get a clear understanding of your current security status. This is best achieved with the help of external security experts who can provide an objective assessment of your security posture. Charterhouse offers a free Cyber Security Review to identify risks and vulnerabilities, and recommend strategies for enhancing and automating your security systems.

FREE Cyber Security Review from Charterhouse

The Charterhouse Cyber Security Review gives an invaluable insight into your business's security posture. Conducted by one of our **cyber security** consultants, the assessment is quick to execute, free of charge and includes:

- Identification of your current security gaps and vulnerabilities
- Assessment of your financial, operational and reputational risks
- **Cyber security** checklist and roadmap tailored to your business
- Step one to developing your automated protection system

Register for your FREE Cyber Security Review here

04 About Us

Who are Charterhouse?

Charterhouse deliver technology solutions that drive business success. Since our inception over 25 years ago, internationally renowned organisations have trusted us to design, provision and support the technology that underpins their operations.

Our security solutions help businesses to protect critical data, users and customers, and to achieve and maintain compliance. We can help you identify your security vulnerabilities and integrate a range of technologies to help mitigate the threat of security breaches.

Our security expertise covers every enterprise requirement, from network security, mobile security and security consulting to compliance and governance.

Our Approach

Our consultant-led Cyber Security Review provides a tailored security profile that pinpoints vulnerabilities and risks, and defines a roadmap to optimise your business security.

Powerful Partnership

We hold close relationships with leading partners such as Palo Alto Networks, Darktrace, One Identity, Cyberscore and Nuix. This enables us to offer a breadth of security and compliance integration unrivalled in the market.

Cyber Essentials Plus certified

Charterhouse are certified members of Cyber Essentials Plus, a UK Government-backed, industry-supported certification scheme to help organisations demonstrate operational security against common **cyber attacks**.

05 Contact

Our consultant-led Cyber Security Review provides a tailored security profile that pinpoints vulnerabilities and risks, and defines a roadmap to optimise your business.

Huw Allanson
Director of Infrastructure Sales

James Brown
Infrastructure Consultant

Greg Clarke
Infrastructure Consultant

Karl Alderton
Infrastructure Consultant

Charterhouse Voice & Data
The Gate House, 5 Chapel Place, Rivington Street,
London EC2A 3SB, United Kingdom
www.cvdgroup.com

To book a Cyber Security Review, please contact us at:

020 7012 1488
cybersecurity@cvdgroup.com