Cyber Security Review

Our Cyber Security Review helps you identify and mitigate risks whilst safeguarding assets and data. By identifying security-related concerns and assessing the associated risks we can help your company make informed decisions to reduce those risks.

Protecting your business through IT security

Through our Cyber Security Review, you'll gain the power to strengthen your overall security posture, gaining insight into your current security status and helping to prioritise security investments. Whether safeguarding critical data or fortifying your infrastructure and security posture, our dedication ensures that every step aligns with your security objectives. Together, we'll compile a comprehensive security overview, leading to transformative protection.

But my business is Cyber Essentials accredited already - do I still need a Cyber Security Review?

If you need an IT infrastructure beyond basic security measures, with secure data handling, demonstrative compliance (GDPR, UK Data Protection Act, NHS DSP Toolkit), and a robust set of cyber defences to reassure stakeholders, consider our Cyber Security Review. Our review goes beyond the Cyber Essentials accreditation, it ensures your security practices are both robust and adaptive to new threats.

As easy as 1, 2, 3...

The Review Process

Step 1

Understand

We invest time to understand your current security posture and goals. Clarity on objectives is key.

Step 2

Analyse

Evaluation & analysis of the current infrastructure and security products/configuration in place.

Step 3

Identify

Deployment of internal & external scanning agents across the network to pull data and identify any known risks.

Step 4

Learn

Human behaviour remains a significant vulnerability. A brief end-user questionnaire will be used to assess your employee's current security knowledge.

Step 5

Evaluate

We evaluate all of the information we've gathered and compile a residual risk-based report.

Step 6

Present

We present our findings and recommendations to you as part of an open workshop and discuss any next steps.

Q&A Cyber Security Review Process

Q1 What specific aspects of the systems will be reviewed?

All servers, end-user devices, installed software, operating systems, network infrastructure, security measures, back-ups will be reviewed and evaluated.

Q2 What are the key objectives of the review?

The key objectives of the security review is to look at the existing security, its effectiveness and any potential risks with the view of making enhancements and further protecting data and systems.

Q3 What systems and tools, if any, are required to conduct the review?

As part of the review process, we would expect to run 3 tools:

1. **Network Detective Pro** (requires WMI ports opening on machines or running individually on a small number) – this collects information on the network, software versions and device security in place.

2. **Internal/external vulnerability scanner** – this scans internal and external endpoints to look for vulnerabilities.

3. **Penetration test tool** – to take vulnerability scanning a step further, we run an internal and external automated penetration test in line with the MITRE ATT&CK framework to highlight known issues that could be exploited. This will be completed using a CREST approved tool.

We can provide Network Detective Pro for existing IT to run in advance of the visit and provide the output files. All of our tools are none destructive to existing systems.

Q4 Are any specific permissions or credentials required for accessing systems?

We would require ‘Temporary Admin Access’ to servers, hypervisors, routers and wireless to check existing configuration and global admin to Microsoft Office 365.

Q5 What information or documentation should be provided beforehand?

It would be useful to have an overview of what your IT estate looks like with access to network diagrams if available.

Q6 What specific recommendations or insights will be included in the report? How will they be specific to the needs and goals of the business?

The report includes best practices for each analysed area and provides a residual report based on the inherent risks and the measures in place to mitigate them. We aim to understand your business goals and any accreditations you may require in order to increase the overall security posture of your organisation.

Q7 At what stages of the process will there be communication?

There will be engagement and communication throughout the process from both the Professional Consultant delivering the review along with the Account Manager. This will involve the following:

1. **Initial consultation including introductions and an overview of the review process**
2. **Reviewing the systems with an initial on-site visit**
3. **Ongoing progress updates from the data analysis along with any additional queries that may arise**
4. **A full presentation of our findings and recommendations**
5. **Agreement of any follow-up actions based on the findings of the review**

Key deliverable dates should be set and agreed upon during the initial meeting, including deadlines for end-user feedback and the presentation date. Typically, we aim to complete the process and present findings within 4-5 weeks from the initial on-site visit.

Q8 Is the information accessed and presented protected under NDA?

In accordance with our security protocols and ISO standards, we ensure that a mutual Non-Disclosure Agreement (NDA) is signed before commencing any work. This NDA guarantees the confidentiality of any accessed or presented information under an official, legally binding document. CT will provide a copy of the NDA prior to starting the service.

5 ways you can boost your Cyber Security

01 Keep your devices up-to-date

Updates for devices and softwares often contain new features, fixes for bugs and performance improvements. They may also contain security patches that will fix known flaws that would otherwise leave your devices vulnerable.

02 Firewall protection for network traffic

A firewall is a network security device that monitors incoming and outgoing network traffic and decides whether to allow or block specific traffic based on a defined set of security rules.

03 Control who has access to your data

Controlling access is a way of guaranteeing that users are verified and have the appropriate access to company data. Access control is a selective restriction of access to data, without authentication and authorisation, there's no cyber security.

04 Be aware of suspicious emails and pop-ups

You can lower your risk of cyber attacks by being vigilant of suspicious emails, pop-ups or links that could leave your device compromised to malware and other viruses. User-awareness training could help with this.

05 Secure device settings

To keep your information secure from potential risks, it's important to review the security and privacy settings on all of your devices, accounts and apps. You should only install trusted software and restrict those able to install software or change device settings to keep your settings secure.

Contact us today to help secure your business

T | 01246 266 130
E | info@ct.uk

ct.uk