Services
Cyber Security Posture Review

Cyber Vigilance
We've got your back...

The Review

Failing to identify and mitigate risks leaves companies extremely vulnerable to cyber-attacks. One data breach can cause an immeasurable amount of damage to your clients' reputation, brand, and customer confidence, as well as involve significant costs in terms of money and time, not only to remediate the threat, but also from employee downtime and lost productivity. Add to that the possibility of large fines from regulatory authorities for non-compliance and you can quickly see why managing an organisation's cyber risk is so important.

The Cyber Security Posture Review helps organisations to understand their current maturity, identify risks and receive actionable recommendations all mapped to the National Cyber Security Centre's "10 Steps to Cyber Security". This ensures that organisations are operating an effective cyber security framework against the ever-evolving threat landscape.

Through a combinations of questionnaires, interviews and follow ups, your organisations maturity is examined to identify gaps and to be provided with contextualised recommendations. This approach ensures organisations have the foundations to defend against cyber security risks and to protect information relating to its customers, employees and business operations.

Key Benefits

▷ Benchmark your current cyber security maturity.

▷ Identify gaps and vulnerabilities with prioritised and actionable recommendations.

▷ Align security to industry best practice and comply with international security standards.

▷ Understand the roadmap for future areas of review and improvement.

▷ Completely independent review which can be tailored to your business requirements.

The Approach

Firstly we work with you to understand your business' services, your assets and how you interact with customers and third parties. Then you will be walked through the "10 Steps and Cyber Security", ensuring you understand the scope of each and are able to identify the appropriate stakeholders for questionnaires and interviews.

Your organisation's maturity level will be determined by reference to a Capability Maturity Model, based on an industry standard methodology. The findings are then formalised in a written report, which provides you with your maturity score and prioritised recommendations in order to fast-track your maturity.

Interested?

Register your interest by emailing us at **info@cybervigilance.uk**. A member of our team will reach out to show you how easy the process can be and how the Cyber Security Posture Review can benefit your organisation.

Prefer to speak to us straightaway? Just give us a call   **+44 (0)1483 948090**

10 Steps to Cyber Security

1. Risk Management Regime
Assess the risk to your organisation's information and systems with the same vigour that would be used for legal, regulatory, financial and operational risks. To achieve this there needs to be a Risk Management Regime embedded across the organisation, supported by the board and senior managers.

2. Secure Configuration
Apply security patches and ensure the secure configuration of all systems is maintained. In addition, create a system inventory and define a baseline build for all devices.

3. Network Security
Protect your network from attacks. Defend the network perimeter, filter out unauthorised access and malicious content. Monitoring and testing security controls.

4. Manage User Privileges
Establish effective management processes and limit the number of privileged accounts. Limit user privileges and monitor user activity. Control access to user activity and audit logs.

5. User Education and Awareness
Produce user security policies covering acceptable and secure use of your systems. Maintain the awareness of cyber risks.

6. Incident Response
Establish an incident response and disaster recovery capability. Test your incident management plan and report criminal incidents t law enforcement.

7. Malware Protection
Produce relevant policies and establish anti-malware defences across your organisation.

8. Monitoring
Establish a monitoring strategy and produce supporting policies. Continuously monitor all systems and networks. Analyse logs for unusual activity that could indicate an attack.

9. Removable Media Controls
Produce a policy to control all access to removable media. Limit media types and user and scan all media for malware before importing onto the corporate system.

10. Home and Mobile Working
Develop a mobile working policy and train staff to adhere to it. Apply the secure baseline and build to all devices. Protect data both in transit and at rest.

Interested?

Register your interest by emailing us at **info@cybervigilance.uk**. A member of our team will reach out to show you how easy the process can be and how the Cyber Security Posture Review can benefit your organisation.

Prefer to speak to us straightaway? Just give us a call   **+44 (0)1483 948090**