Remote Working Security Health Check Service

Organisations are hastily reacting to employees working from home (WFH) and risk overlooking security requirements for remote working. Cyber criminals are actively exploiting this opportunity.

We offer a range of security health checks to ensure you are meeting security and regulatory compliance standards, no matter where your team are working.

Microsoft 365 Security

With the increase in remote work, companies will have to prepare in various ways to avoid cybersecurity risks or interruptions to business. When supporting a remote workforce, security controls shift. Microsoft's Office 365 offers a great selection of core security features to help protect your business.

Challenge

Due to the COVID-19 pandemic and resulting lockdown, businesses implemented remote working solutions and adopted cloud services such as Microsoft Office 365. The rapid nature of these deployments has meant that best practices weren't followed, insecure or misconfiguration was applied or security controls may not have been fully introduced. The result has the potential for lowering overall organisational security. C5 advises all organisations to make sure that their infrastructure assets are protected against attackers who could take advantage of misconfigured Office 365 installations during this period.

Recommendation

C5's certified Microsoft 365 Security consultants will ensure your Microsoft 365 cloud environment is configured in line with Microsoft's best practice guidelines. We will provide a report on key findings with actionable items to help enable your employees to work more securely.

Microsoft 365 Health Checks

- Run an Exchange Online Protection Baseline and make recommendations
- Review and if required enable additional alert policies and Audit Log search
- Review Admin Consent Requests to prevent users from inadvertently granting permissions to hostile third-party applications
- Advise on Multi-Factor Authentication (MFA)
- Verify and rectify any issues with your current Email Authentication to help protect against potential spam, malware and phishing

Cyber Essentials Gap Analysis

Cyber Essentials (CE) is a Government backed scheme that provides simple but effective measures to protect against a wide range of the most common cyber security attacks. By adhering and certifying your company against the Cyber Essentials Framework you have the peace of mind that your defences will protect against the vast majority of common cyber-attacks.

Challenge

With the increase of remote working, security boundaries to your company's IT infrastructure are changing. Commonly the edge of your network is your first line of defence, however now that users are working remotely, they and their remote workstations become the edge of the network. Coupled with rapid change to facilitate the ability to work in this new way, it becomes a challenge to keep up adherence to the Cyber Essentials Framework.

Recommendation

C5 offer a Gap Analysis service against the Cyber Essentials Framework. Our Security Consultants have vast experience working with the CE framework and through interviews and some light hands-on technical checks, we can provide a report of gaps against the CE framework, We will also provide recommendations for remediations if you are not adhering to the correct level of security.

Cyber Essentials Health Checks

- A report of your gaps in adherence to the Cyber Essentials Framework
- A proposal to remediate any gaps in adherence to the Cyber Essentials Framework
- We will assess your company's adherence to the five domains of cyber essentials: Office Firewalls & Internet Gateways, Secure Configuration, Software Patching, User Accounts & Malware Protection

Remote Access Services

Businesses have delivered tactical IT solutions to ensure that their users can continue to work from home during the COVID-19 pandemic, with a variety of remote access solutions. Many of these solutions have been implemented in a rush with systems that have not been designed or configured to accommodate the influx of remote workers.

Challenge

User experience is key for engagement and productivity; users become frustrated when they experience slow applications and sporadic connectivity. The business has expanded its footprint operationally while managing and protecting additional endpoints. IT teams now need to support whole companies of employees who now work remotely, battling their unique home networks, over-utilised firewalls and saturated internet connections.

Recommendation

C5 offer a service to enable performance monitoring of your remote working solutions to ensure that user experience is optimal and can provide a report on key findings with actionable items to help enable your employees to work effectively.

Remote Access Health Checks

- Highlight slow performing applications, slow logons, problematic home networks, endpoint configurations and supporting network infrastructure
- Chart the user experience and quality time in which they have access to the systems that they need to perform their tasks
- Advise on recommendations to any highlighted issues to ensure you achieve the desired performance of your remote workers

Bring Your Own Device (BYOD)

Traditionally Remote Workers only made up 3.2% of the entire workforce and 44% of companies didn't allow remote work at all. Natural disasters, sick dependents and state of emergencies happen but today's COVID-19 scenario is unprecedented.

Challenge

Due to the COVID-19 pandemic and resulting lockdown, businesses rapidly implemented remote working solutions. With the sudden requirement for all staff to work remotely, businesses were left with a shortage of corporate devices to access their data and some organisations hurriedly implemented remote access solutions that used a BYOD approach for accessing company data.

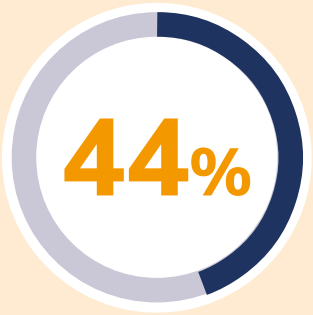
Recommendation

C5 will complete a health check of the solution that you have implemented. We will review BYOD and acceptable use policies and ensure they are aligned to your implemented solution. We will also review your controls in place and provide recommendations on any gaps in your security posture.

BYOD Health Checks

- Review BYOD and acceptable use policies
- Discuss and review remote access solutions in-use
- Review OS and application patch management settings
- Review of presence of endpoint security
- Provide guidance on GDPR conformity for data handling

Traditionally Remote Workers only made up 3.2% of the entire workforce



Until recently 44% of companies didn't allow remote work at all

Collaboration

With the increased need for staff connectivity and collaboration, driven by both changing business needs and the current health situation, more and more organisations have rapidly implemented Microsoft Teams – some overnight.

Challenge

Hackers and malicious actors are operating as usual and are ruthlessly taking advantage of the current uncertainty. Some going so far as to actively hack hospitals for ransom.

Recommendation

We offer a rapid and fully remote service in which we review your key Microsoft Teams security settings and advise whether they are configured in a security conscious way. You may want this service to ensure that your Teams activity (e.g. meetings, files and conversations) is secure or simply to gain piece of mind which comes by having an independent party providing a view on your arrangements.

Collaboration Health Checks

- Review your main MS Teams configurations related to your security posture
- Observe 56 configuration settings (out of which 32 are policies and 24 are settings)
- Indicate the security risks you may be exposing yourself to and how to minimise such risks

General Data Protection Regulations (GDPR)

Remote working and the use of personal devices in a non-office environment significantly increases the risk of fragmented data storage, and compromised data integrity, accuracy and security. We know that human error is the cause of most breaches and the stress and unfamiliarity of the COVID situation will increase this risk.

Challenge

The risk of data breaches is increased and the GDPR principles become more challenging to adhere to with the associated risk of fines from the regulator and reputational damage.

Centralised data management becomes problematic as staff are physically scattered and data may end up being stored locally on insecure devices or transferred in insecure ways.

Recommendation

We can provide a wrap-around solution for your information management, providing you with 'a single version of the truth' for your data in a secure location with locked down permissions. We can also provide bespoke advice as to the right third-party solution for your encryption challenges. In terms of governance we can assist you with rolling out best practice BYOD and acceptable use policies to ensure any audit of your information governance is bullet proof.

We can provide any necessary training for staff to fill any knowledge gaps. Alternatively our outsourced DPO service can deal with your data breaches, subject access requests and DPIAs in this challenging time.

GDPR Health Checks

- Review your existing information management system and check its security and adherence to the data protection principles
- Review your information management policies and risk assessments
- Analyse your existing encryption and information security protocols against best practice methodology
- Customised recommendations to reduce your risk of breaches, regulator fines, civil litigation and reputational damage

Our remote working security health check service forms part of our 'Advise, Transform, Run' methodology.

Advise

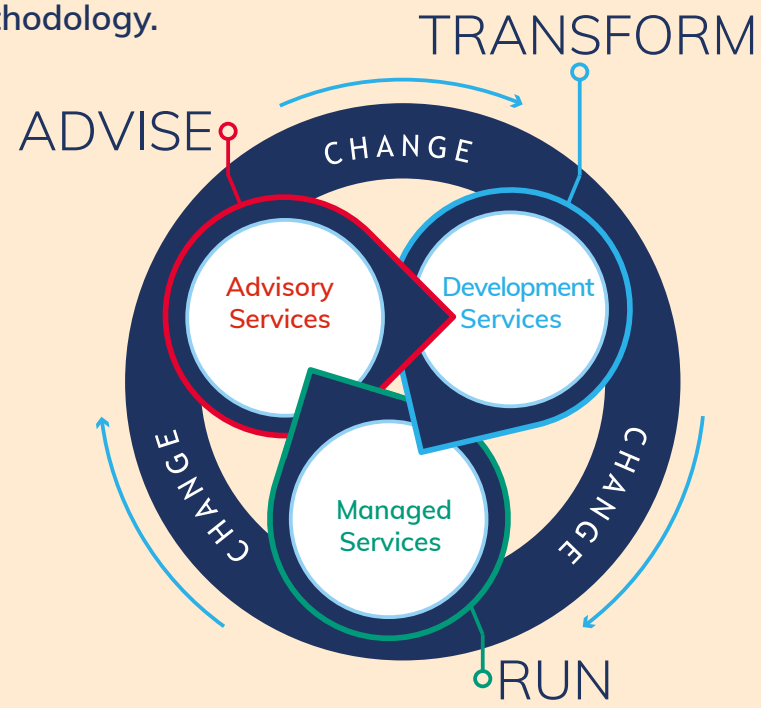
Our Advisory team will complete the health checks to suit your organisation's needs in order to produce a report including recommendations.

Transform

Based on suggested reviews, recommendations and analysis, our team of technical experts can implement solutions to improve your security position.

Run

Supported by a 24x7x365 team, our managed services operation can mange and monitor your security solutions. This will protect your business, even when you are not working.



Our team is here to support your Network and Security needs.
For more information please contact Richard Welsh:
Richard.Welsh@c5alliance.com or call **01534 633733**

www.c5alliance.com