COVID-19

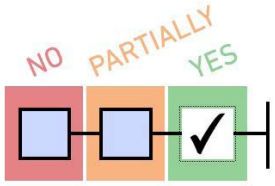
INFORMATION TECHNOLOGY AND CYBER SECURITY CHECKLIST

BEGIN

MAZARS

INFORMATION TECHNOLOGY AND CYBER SECURITY CHECKLIST

This Mazars Information Technology (IT) and Cyber Security checklist provides both IT Managers and Senior Management with the ability to conduct a quick review of the critical areas concerning IT operations and security within your organisation in the difficult circumstances that we are currently operating.



Answer each of the questions in relation to your current IT environment. You can check the box beside each question which best describes your situation. Where you are answering either Partially or No to any of our questions, you may be exposed to an inappropriate level of risk.

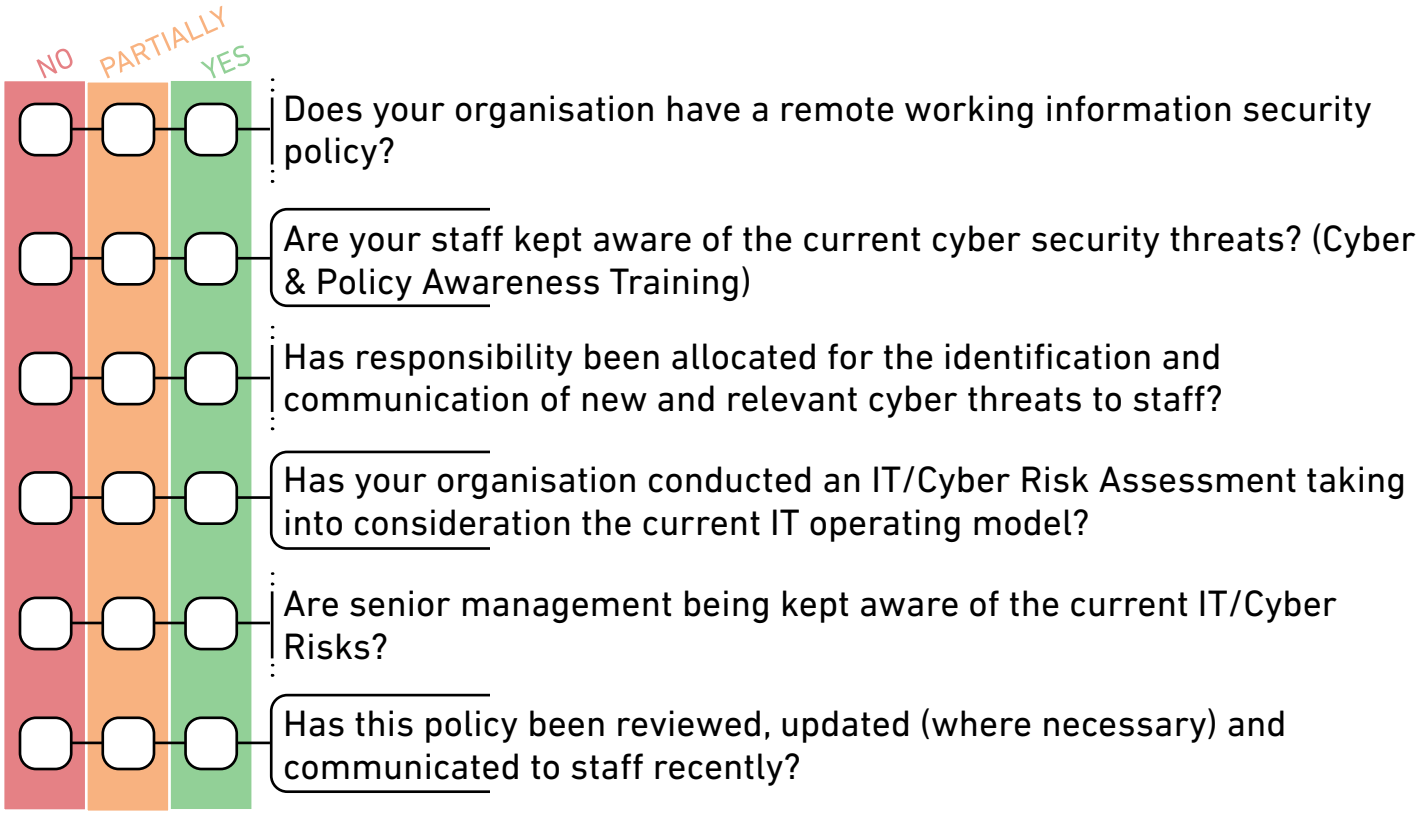
Mazars IT Audit and Security Team can assist you with any of the 10 areas

- Security Policy and Awareness
- Data Privacy
- Remote Access Solution
- End User Devices
- Monitoring
- Third Party Support Providers
- Disaster Recovery
- Cyber Incident Management
- Business Continuity
- Communication

SECURITY POLICY AND AWARENESS

With the changes that COVID-19 has forced organisations to make in terms or your IT operations, and the continuous Cyber Security threats imperative that all organisations ensure that their IT Security policy includes remote working requirements and that all staff maintain an awareness of the current cyber security threats.

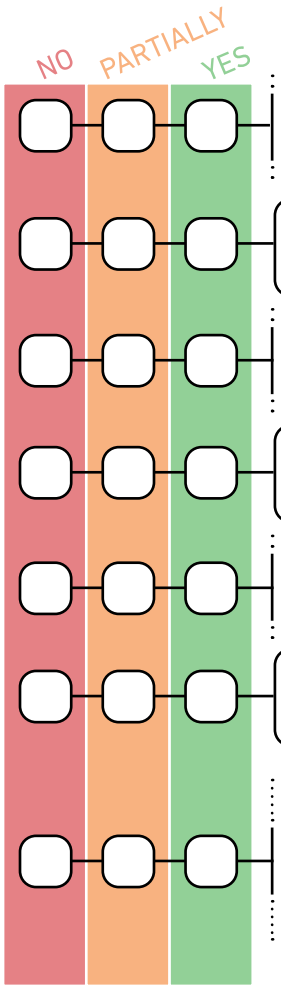
Senior Managements understanding and oversight of the IT and cyber security risks that an organisation is exposed to has never been so important.



DATA PRIVACY

Covid -19 has not changed organisational regulatory requirements in relation to protecting the privacy of personnel data.

Organisations will have introduced new approaches to the way that they process personal data. It is every organisations responsibility to ensure that all personal data is adequately protected.



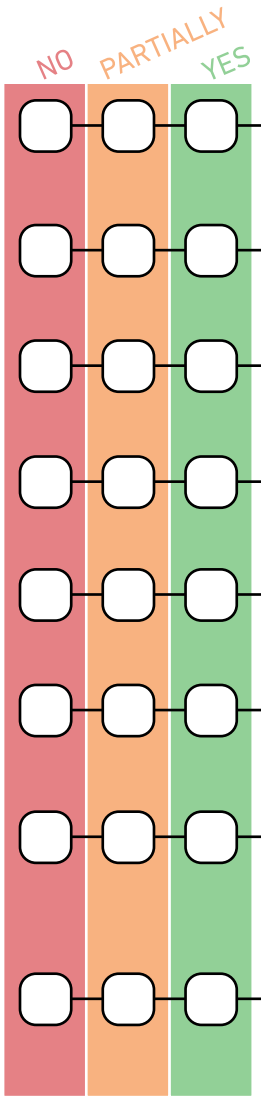
- Are staff clear on who to report a data breach whilst working from home?
- Are personal email accounts being used for business purposes?
- Are controls in place to monitor for the use of personal email accounts and auto forwards?
- Has data privacy controls to minimise data leakage of personal or business information been put in place e.g. data loss prevention?
- Are technical controls in place to restricted personal data from being copied to personal devices when working remotely? (Citrix)
- Are controls in place to restricted personal devices used for remote working from being shared?
- Has remote working altered the way that you process personal or sensitive categories of data such as the introduction of new cloud based technology? If so, have you assessed the risks via a Data Protection Impact Assessment to determine the mitigating actions?

REMOTE ACCESS SOLUTION

Most organisations are now massively reliant on technical solutions to enable their staff to work remotely. Such tools expose an organisation to a new level of risk. In recent days we have heard of numerous instances where remote working solutions have been compromised by cyber criminals.

The exploitation of security vulnerabilities on remote access may lead to unauthorised access to an organisations data resulting in a data breach.

How secure is your solution?

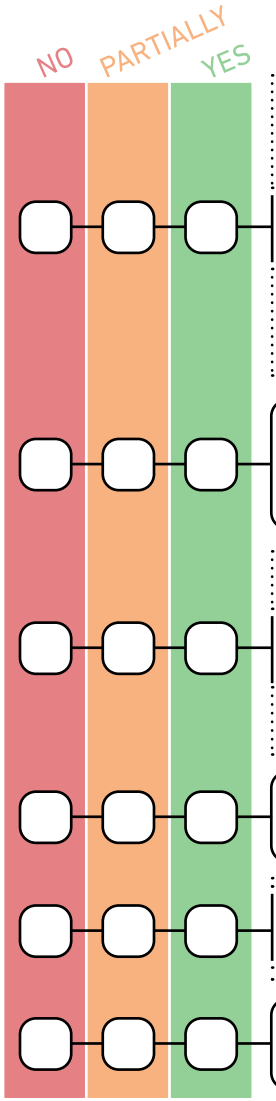


- Do users have remote access to all business critical applications?
- Does the organisation have adequate denial of service protection at a network device and/or ISP level?
- Does the solution require two factor authentication (MFA)?
- Have strong passwords been implemented?
- Does it provide an adequate level encryption?
- Has a network vulnerability scan been conducted for on you firewall and VPN solution in the past 6 months?
- Is your remote access solution kept up to date with the latest security vulnerability patches?
- Does your remote working solution and network infrastructure have the ability provide an adequate business service for a prolonged period of time? (In terms of scaling up connections, licenses, performance and network capacity.)

END USER DEVICES

Securing a desktop device within an office has become normal practice. However, COVID-19 and the need to work from home has presented organisations with the challenge of ensuring that all devices that connect to the internal network and/or process company data are adequately secured.

Do you known how your staff are connecting to your network?



Have the organisations laptops and remote devices been security hardened prior to issue? For Example:

- Encryption
- Anti virus/malware solution
- Up to date security patches
- VPN client installed
- Lockdown of use of USB storage devices

Does your organisation have central management tools in operation to ensure that all remote workers laptops/remote devices are kept up to date with the latest anti-virus and vulnerability patches?

Are security controls in place at the gateway to ensure that devices that connect to the organisations network are adequately protected (Network Access Controls)? In relation to:

- Up to date security vulnerability patches
- Anti-virus/malware protection installed and up to date

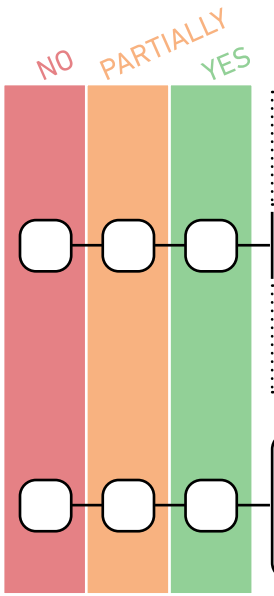
Are staff required to use secure network connectivity when working remotely?

Is web filtering in place to restrict the use of none approved remote working/ conference applications?

Have you requested that staff members turn off voice recognition software and device in the facility of the working environment at home.

MONITORING

Most organisations have or are close to the end of implementing their remote working solutions. In order to sustain these solutions and ensure the availability and security of an organisations systems and data. IT Managers now need to ensure that they have access to an adequate level of network and security monitoring tools and they are configured to notify staff members and/or third party support providers within an adequate timescale.



Is IT system monitoring and maintenance being conducted at the same level as prior to remote working. Has responsibility for monitoring and maintenance been clearly allocated. In relation to areas? Such as:

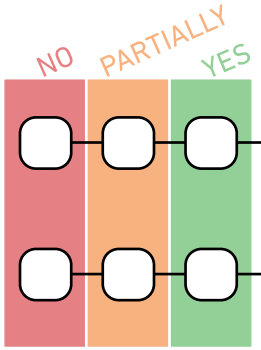
- Backups
- Scheduled Tasks
- Capacity & Performance Monitoring
- Security Monitoring

Whilst working remotely has your organisation retained the capability to identify and react to suspicious network activity within an adequate time scale?

THIRD PARTY SUPPORT PROVIDERS

Third party support providers are experiencing the same level of challenge as all other organisations. If not more as they may be responsible for multiple networks and systems as opposed to one. As a result, they may not be able to provide the same level of support and monitoring as they may have previously.

How reliant is your organisation on third party support providers?



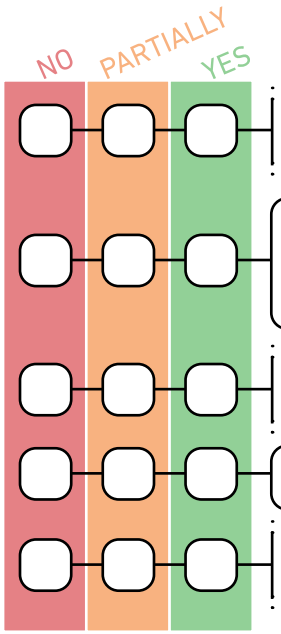
Is your third party support provider able to deliver the same level of service that was provided prior to the remote working?

Have response times and service levels been impacted?

DISASTER RECOVERY

Disaster recovery remains a key area for all IT Managers, ensuring that they have access to all the system monitoring and management tools and can conduct restoration tasks remotely if required.

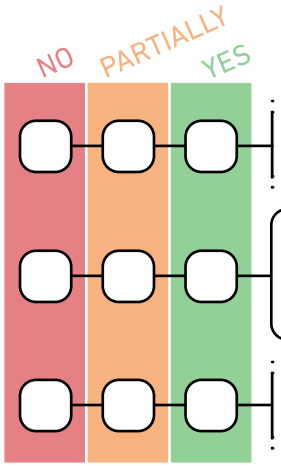
Have you identified all of your critical assists and are they adequately protected?



- Does your organisation have a documented technical disaster recovery plan?
- Has your organisation retained access to all of network management tools required to assist in the management and remediation of a system and/or hardware failure? (where possible)
- Are controls in place to ensure that all remote workers critical data is being stored in an area that is being backed up on a periodic basis?
- Has your organisation identified all of its IT assets?
- Are all critical assets configured to ensure their confidentiality and availability?

CYBER INCIDENT MANAGEMENT

The introduction of remote working has made the management of a cyber-attack significantly more difficult. Current trends indicating a rise in sophisticated cyber-attacks on organisations of all sizes. As a result, the development or updating of your cyber incident management is required.

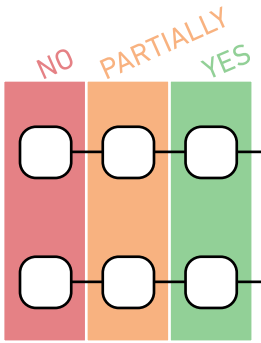


- Does your organisation have a Cyber Incident Management Plan?
- Has the plan been updated, tested and communicated to relevant staff to prepare for cyber incident response whilst remote working?
- Do staff know who to report a security incident?

BUSINESS CONTINUITY

As no one knows how long we are going to be exposed to these challenges' organisations need to start to consider how they are going to sustain operations for a prolonged period of time. The following questions should be asked: Are the current arrangements adequate to keep the organisation going for 2-3 months?

What will your organisation need in place to ensure that all its critical business processes are kept operational?

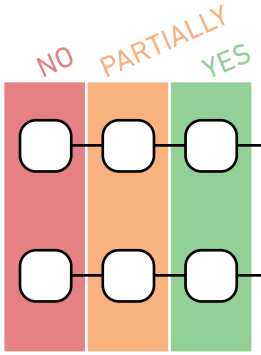


- Has your organisation conducted a business impact assessment to identify any critical business processes/infrastructure/applications current/future that may require additional IT services and/or capacity?
- Has a plan been developed and tested to address all critical business requirements whilst the organisation is remote working?

COMMUNICATION

The ability to communicate both internally and with your clients is key to an organisations success going forward.

Does your organisation haveadequate solutions and network connectivity to service your organisations need? Is the solution that you have selected secure?



- Has your organisation a secure communications tool to enable conferencing and screen sharing with colleagues and customers/clients?
- Do you have adequate network bandwidth to cope with the increased use of online conference solutions?

CONTACTS

ALEX BURNHAM
Director, IT Audit & Security
aburnham@mazars.ie
087 6958135

SARAH HIPKIN
Director, Consulting - Data Protection
shipkin@mazars.ie
087 7387387

www.mazars.com

MAZARS