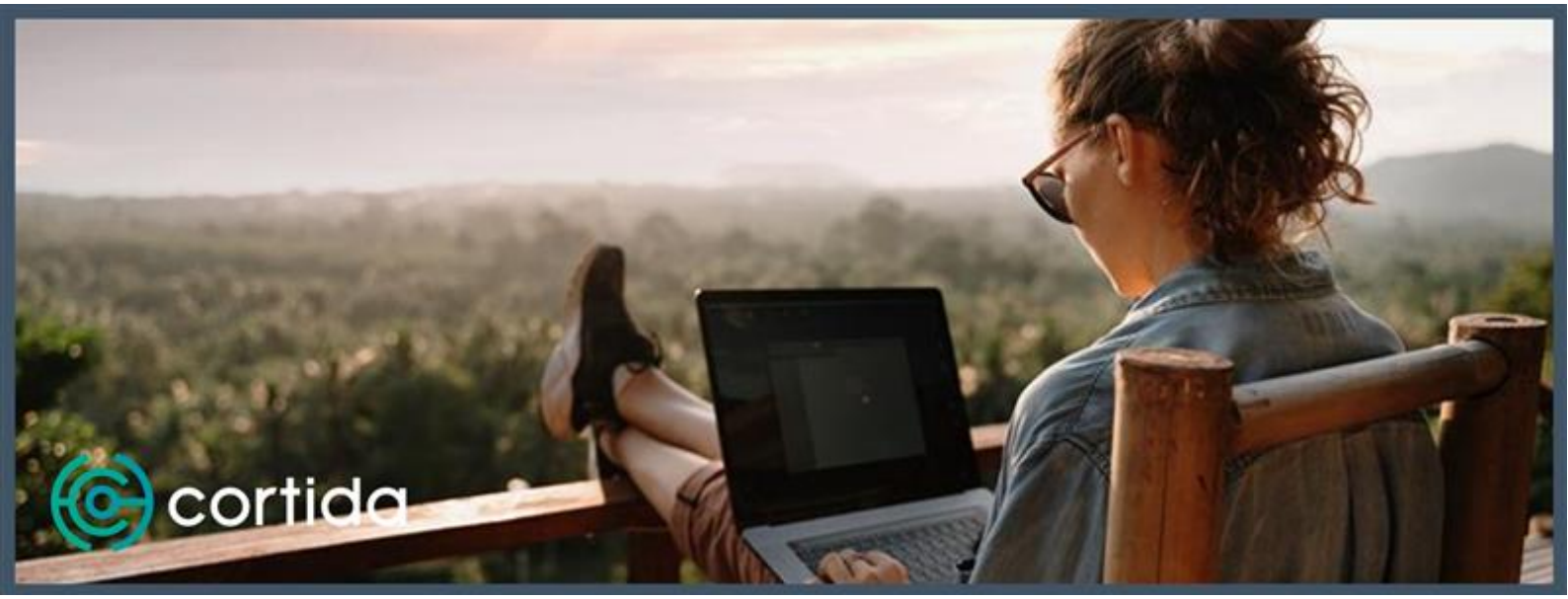

Preparing your Organisation for Secure Remote Working

March 2020 saw reams of businesses close their physical doors and retreat to the safety of remote working, the extent of the remote working requirement presents new challenges to the safety and cybersecurity of your organisation.

Your business is most likely already online, but the pandemic has created a predominantly digital, remote workforce overnight. More remote users, more digital devices, more remote risk. As you open up resources to support your clients, staff and business throughout the Coronavirus crisis – you rely on a multitude of variables that without proper management, leave your networks, data and organisation vulnerable.

Applying a structured approach can strengthen your cybersecurity posture and protect your remote operation, thereby reducing your exposure to cybercrime. Three primary approaches should be considered when moving employees from a protected internal corporate network to working over the public internet. A **strategic** approach that applies to upper management and deals with governance. The **tactical** approach that deals with what IT and security specialists need to consider as they implement new solutions. And the **people** approach that provides sensible ways of dealing with new working conditions that all staff should be aware of.

Strategic: Preparing for remote working

The themes of the strategic approach include understanding risks, ensuring confidential or sensitive data sits in centralised systems (rather than a user's own devices) and ensuring data access is managed and follows a principle of least privileges. Equally important is the need to implement a solution that can apply centralised management of user devices to reduce the likelihood of risk. Finally, providing clear guidance on what rules should be applied to remote working is essential. Each is discussed at a high level below.

Risk Assessments - Conduct a risk assessment that considers what data needs to be exposed over public networks, who needs access to it, what security measures are required to protect it and whether they already exist. With an elevated understanding of the risks, it is possible to determine risk treatment options which may include tolerating, transferring, or treating the risks.

Centralised Management - Take positive action and use tools that provide centralised access to files and other network resources that can enforce security management regardless of the user's location. Examples of solutions that can centrally manage security in remote working include:

- **File and email management** – Providing a remote access environment such as Office 365 or Google allow your organisation to ensure staff sync files or emails back to a secure location which is protected by backup and encryption.

- **Identity and Access Management (IAM)** – IAM ensures networked users are allowed access to only the resources relevant to their role and authority. It is essential to ensure the principles of IAM are applied and maintained regardless of whether a worker is based in the office or remotely.

- **Mobile Device Management (MDM)** - Such solutions provide centralised provisioning and enforcement of your company's security policies against devices that will be used away from the office.

Formal remote working policies – Ensure your company's rules for home working are formalised via a policy that everyone has read, understood and agreed to. The policy should be clear, unambiguous and allow your employees to understand the risks and consequences of not adhering to them and explain that compliance will be monitored. It should be explicit about what devices can be connected to the network and that devices may not be shared or used by other family members.

Incident preparedness – Ensure your organisation has an up-to-date incident response plan; that it includes remote working scenarios and has been tested to ensure it can be followed in the event of a data incident.

Tactical: implementing and managing remote working.

The urgent requirements for remote working have seen some heroic and agile efforts undertaken by IT and security teams who have managed to respond to meet the need. However, in the absence of the right company strategy (discussed above) they have often been torn between the demands for rapidly deployed remote access to data and systems, and the requirement to keep them confidential, reliable and available. In these stressful situations, it is important to remember that organisations have ethical, contractual and regulatory obligations for protecting systems and data.

So, beyond being given the task to implement the organisations risk assessed and centralised vision of remote working; IT & Security teams must be provided with resources, authority and visible senior management support to complete the task, without which, the effectiveness of their people, process and technology measures may be constrained with potentially disastrous effects.

With processes and projects sanctioned, IT & Security teams can focus on implementing the strategic processes and technologies whilst ensuring tactical deployments are used in harmony to maximise security.

Possibly the most important implementation strategy is centralised provision. This requires security to be mandated by pushing it down to remote teams, rather than relying on users to do the right things.

The following centrally managed policies and configurations are a good starting place for managing remote devices:

- Enforce the removal of default anonymous accounts and shared passwords so attackers can't guess possible logins.
- Enforce strong password so that all passwords are impossible

to guess, and are changed regularly.
- Centrally enforce the application of patches and security updates.
- Centrally deploy and manage anti-virus and endpoint protection.
- Centrally enforce enabling of a local firewall to block incoming connections.
- Configure devices to automatically lock after a period of no use.
- Disable external interfaces such as USB accessories.
- Implement application whitelisting that restricts the applications users are allowed to install and run on their devices.

Beyond centralised management, corporate IT and security teams should implement corporate-wide security controls to protect in-flight and at-rest data. A virtual private network (VPN) should be used to protect in-flight data and as a minimum, the VPN should be implemented by the organisation and include encryption and Multifactor Authentication (2FA), that:

- Hides the user's IP address
- Encrypts data transfers in transit
- Masks the user's location

Data at rest should be protected by device and server encryption technologies and by removing administrative features from all computing equipment for general users, you ensure that access to data is limited to those with a legitimate business need.

Video conferencing can also impact the security of data in flight, so the solution used should be risk assessed, provisioned by the organisation and have default security settings such as multi-factor authentication, encryption, and a lobby function to control access by guests.

People: The responsibility of individual users

The strategic and tactical elements discussed in the earlier sections cannot be met solely through the application of policy and technology. They also rely on employees. Employees are commonly targeted by cybercriminals who seek to leverage the reality that humans are fallible, make mistakes and at this time may be more easily distracted by unusual working conditions.

By securing your employees, your organisation has a greater chance of protecting your data and systems. To secure your employees and therefore your company, organisations should ensure that their human firewalls (first line of defence) understand their critical role in protecting data and systems and the good practices they should follow.

Important security practices that remote users should be aware of:

Public Wi-Fi - Avoid using public Wi-Fi in café's and other public places - use a personal mobile hotspot instead.

VPNs – Do not disable the company supplied VPN that protects connections on public Wi-Fi.

Home router security - For home working over a local private Wi-Fi connection, reset the default Wi-Fi router password to something that meets the organisations password complexity policy.

Sharing devices - Never share corporate devices or access to systems and data with anyone else.

Look after devices - Never leave devices or laptops in the car or unattended and always lock them.

Reporting - Know how to report any theft, loss, or suspicious security incidents.

Video Conferencing - When using video conferencing, check your environment to ensure private information isn't visible to observers and if screen sharing, ensure open applications and desktop files do not

expose sensitive information.

You can never entirely remove the threat, but you can defend it, reduce it and demonstrate your regulatory compliance.

To access further guidance contact Cortida here. Cortida is the home of information and cybersecurity risk management. We favour ‘appropriate’ security measures over their costly, convoluted alternatives. Learning and understanding your business, its objectives and your attitudes and appetite for risk mean that we can better protect them. We measure how data supports or threatens your objectives and dismiss any unnecessary and costly audits of your security. Our focus is reliability, technical expertise, a personable partnership approach and delivering tangible value to your organisation. This allows us to identify, understand, reduce and manage your security risk.

The Cortida partnership approach:

- Establishes an understanding of your organisation’s objectives and attitudes towards risk
- Assesses your organisations data to determine its importance and value and need for protection
- Includes a reasoned assessment of the risk, based on probability and likelihood of loss or incident
- Formally identifies an appropriate security benchmark along with any gaps between the in-place measures and the target
- Provides a clear understanding of what needs to be done and in what priority

Want to understand more about this subject ? Get in touch at info@cortida.com

+44 (0) 207 164 669
info@cortida.com
www.cortida.com
150 Minories, London, EC3N 1LS