SECURITY AND NETWORKS

REMOTE WORKING CHEAT SHEET

During this unprecedented time, WM and Net Reply offered guidance in a webinar around considerations and possible changes businesses may need to address with mass remote working. In addition, Net Reply would like to provide a cheat sheet of key Security and Network topics discussed during the webinar. Please understand, there are many additional factors to consider when embarking on a remote working strategy, the focus of this is to minimise disruption as staff continue to carry out their duties whilst everyone works remotely

In general we are attempting to ensure the following high level measures:

- Ensure infrastructure maintains consistent availability for staff use
- Ensure data remains secured and the business maintains control of PII and sensitive data
- Maintain the ability to operate and escalate problems in a decentralised staffing model
- Adapt procedures to fit staff working environments instead of trying to adapt staff's home environments to fit an existing process

Security Considerations		
Do your Security Patterns and Policies allow all types of business tools to be accessed remotely?	Identity Management	Review to understand whether and how best to maintain security whilst allowing business productivity
		Applying stronger Identity Management if relaxing device type or location is necessary - Applying MFA and other additional Access Controls
		Apply different rules for non-business sensitive systems
		And stricter for systems with sensitive or PII data
Access Control	Conditional Access increases flexibility	Control ability to access information based on their location and device type
		Depending on the type of data users are accessing - own saved files - business critical systems and PII data
		Control ability to view / edit / delete based on device used
Device Management	BYOD Management	Consider Mobile Device Management (MDM) & Mobile Application Management (MAM) services
		It's imperative more than ever to maintain up-to-date software
		Review of Endpoint Protection - use AI driven EDR solutions in addition to AV services
		Ensure business devices are healthy, run assessments on BYOD devices
Compliance & Auditing	Do any systems require routing via certain network points for compliance & auditing purposes?	What controls do Service and Security Operations teams use?
		Where does the business audit their business applications?
	Secure in transit	Is there enough provision of VDI services for business critical applications access if not allowed externally? It's easier to maintain control of sensitive data using VDI solutions
		Ensure applications use natively secure channels, or run over a secure (VPN) tunnel
Service / Security Operations	Staff cannot always easily re-create their work environment.	Work to adapt working processes, rather than the home-work environment. Divide Service Management and SoC teams so Sub-teams focus on certain areas
		New ways of working will likely need to be established - increased regularity of meetings and channels to help with escalations, supporting close collaboration in a decentralised manner
	Reminding staff of threats and ways of working	Expect a rise in phishing attempts, remind staff to remain alert to external threats
		Staff using non-standard solutions without an audit trail
		People trying to "get things done" which may not fit with the business's standards
		Are staff aware of how to reach the relevant team for assistance if they are unable to access systems, report outages, password reset etc?
	Disaster / Recovery	People - if a significant amount of staff fall ill - ensure the business has coverage of roles
		Systems - ensure the right processes to manage disaster situations are in place
		Think about how to provide replacement devices and hardware for new starters

Network Considerations		
Can your infrastructure cope with 100% Remote working? These Services could suddenly be put under enormous strain due to the load of the entire business using them	Who needs to connect via VPN?	Consider which Services then which Departments?
		Are VPN Clients deployed on all systems?
		Give guidance around when staff should use VPN services whilst working remotely
	Can all services be accessed remotely? Without VPN or with?	Split tunnel may alleviate strain on network infrastructure rather than full VPN?
		Review of networks within the Split-VPN service
	Reducing VPN Usage	An alternative to VPN are Proxy services for applications that alleviate the need to connect via the VPN.
		Review VPN Policies to ensure Idle VPN connections are dropped after a given time to reduce concurrent connections.
		Review of VPN client licenses to ensure enough licences are provisioned for remote workforce.
		Businesses who have moved to public cloud and proxy services mean the majority of staff may not even need to use the VPN service
Do all your staff have Laptops or mobile devices capable to carry out work activities?	For staff who have desktops can laptops be provided / provisioned?	Can Mobile devices be used?
		Can BYOD be used?
Are your staff able to work from home?	Home Broadband contention. With other family members / house mates also at home	Enough bandwidth for work related Voice / Video / Desktop Share / VDI sessions, round trip sensitive applications?
		Likely increase of Mobile data (tethering) and mobile calls.
		Recommend using wired connection to routers where possible
	Have staff worked from home previously	Are staff setup with the correct home office equipment? If businesses require staff to work from a home office the business still has a responsibility to provide a safe working environment. Think Headset, Chair, Monitor, Mouse, etc
		Some employees may not have worked from home before and will need support and guidance. Some employees will feel like there's information overload so there's a delicate balance
	Redundant Connectivity Methods	Can staff remain connected if their broadband is down? Provide guidance around 4G/5G mobile data dongles or tethering from mobile devices

NET REPLY

Net Reply is the Reply Company specialising in Networks and Security. With an agile and collaborative approach we partner with our clients to ensure their network ecosystem is ready to exploit the opportunities of Digitalisation, IOT and Cloud by harnessing the power of Automation and Future Networking. Our Security Practice provides an innovative and pragmatic approach to help our clients understand the threats to their business and to manage and mitigate service and privacy risks, leveraging the latest machine learning and automation technologies. Founded in 2010, Net Reply is a focused, dedicated, agile group of talented and experienced technologists and consultants. www.net.reply.com