Technologies (Pty) Ltd
INFORMATION TECHNOLOGY SPECIALISTS

Whitepaper

6 Steps for Effective & Secure Remote Worker Readiness

An A-to-F checklist that's easy to implement

Remote Working on the Rise

COVID-19 has created an immediate need for employees to work from home, as global lockdowns and mandated social distancing have kicked-in to protect individuals and curb the spread of the pandemic. It is now crucial for organizations to provide employees with productive and fully secure work-from-home (#wfh) environments. Doing so requires implementing a remote worker strategy that includes the necessary security, policies, tools, system-access, training, equipment, and appropriate connectivity. Organizations must also continuously review and fine-tune their remote worker strategies to ensure ongoing effectiveness.

Why is this Simple Checklist Needed?

From a data security perspective – and for businesses in many industries, regulatory compliance makes it crucial to protect your systems from attackers and mitigate the risks that data breaches pose to your customers and your organization. At the same time, small and medium-sized businesses are at just as much risk as larger organizations and must make the most of the resources they have available.

This quick and effective checklist – as easy as A-B-C-D-E-F – helps to close security gaps and guide the implementation of solutions and practices that make employee remote work environments that much more secure.

The A-to-F Checklist

A is for Antivirus, Anti-malware, Anti-spam, Apps, Awareness, Assets and Audit:

Make sure the devices your employees use in their remote work environments have reputable antivirus, anti-malware and anti-spam software loaded and working. Ensure these tools are configured for automatic updates and ready to defend your systems from the latest known attacks and exploits.

It's equally important to apply all available application and operating system updates to close those security gaps too. Any apps that employees load onto their computers and mobile devices should also be checked and updated. Apps that have not been frequently accessed and don't add to productivity should be removed to reduce the attack surface. Mobile app permissions are also a key concern, as many apps capture a great deal of personal information from the mobile device. Carefully question the necessity of all present applications and do enforce appropriate security policies.

Nurture employees' awareness about how their actions impact the privacy and security of their own devices and the organization at large. Engage in practical exercises to instil this knowledge across your workforce and continually train employees in best practices.

Perform a device audit to gain a full awareness of the locations and specs of all hardware assets in the hands of your employees containing company data or any that are able to access company systems. This includes (but isn't limited to) desktop and laptop PCs, Macs, smartphones, tablets, and USB storage devices.

In the same way, audit any physical hard copy files that any user might take home with them or maintain in their possession. Use tools to remotely monitor and secure devices and systems.

Maintain the ability to audit these security measures to demonstrate your regulatory compliance easily and more provably if (and when) required to do so. In the aftermath of incidents in which devices are lost, misplaced, or stolen, the ability to prove compliant practices that mitigate the risk of data exposure are crucial in avoiding regulatory action and reputational harm.

B is for Backups and Browsers:

Maintaining regular and automatic offsite backup of company data stored on remote employee-used devices is vital for both data security and productivity. If a system is hit by ransomware that holds your data hostage,an available data backup can become your get out of jail free card.

Employees' web browsers must also be checked to verify security and be regularly updated. Some browsers are more secure than others: make sure the browsers your employees use are not vulnerable to attacks. There are several self-testing tools and web-based services available which can assist in this verification.

C is for Complex-passwords, Clicking, and Communications:

Train and require your employees to use complex passwords to protect their devices. Go a step further by introducing automated tools to enforce complex password requirements and multi-factor authentication as policy. Easily guessed passwords present a much higher risk of unauthorized device and data access. This is a basic but crucial access control security measure to have in place across your entire inventory of devices. Implement complex password enforcement such that you can prove the presence of this security measure on any device to regulatory auditors if the device is compromised, especially on any standalone/workgroup computers not attached to a domain.

Train employees to recognize phishing emails and social engineering attacks. Educate them to avoid clicking on suspicious links or opening attachments from unknown sources. This training must be continuous in order to build employees' capabilities as responsible caretakers of sensitive data and cover secure practices with desktop and mobile device use too.

Employee training should also cover best practices for secure communications, including those across social media, text and email. Any file attachments or public posts must be scrutinized for security risks. Ensure you have the right disclaimers and protections on your communications as required, and use security tools to provide helpful email filtering and warnings against risky social media posts. Make use of a VPN on devices when connecting from any employee-used device to any company networked system

D is for Downloads, Don'ts and Defensive Actions:

Employees must be sufficiently trained to avoid downloads from unknown sources that could put their devices and computer systems at risk.

Training should also cover a clear and concise list of Don'ts – things the users should NOT do. For example, "Don't write down passwords on a sticky note kept with your device" is a good rule to include. These rules should also form the basis for your IT usage and Bring-Your-Own-Device (BYOD) policies.

Have adequate defensive measures in place to protect against unauthorised data and device access. Countermeasures that can work and act independently of a network connection, including "quarantine" functions that cut off access to data (or the device itself) can prove very valuable in mitigating data exposures. These capabilities effectively secure data even when a device is compromised, stolen, or an employee becomes an unauthorised ex-employee.

E is for Encrypt and Educate:

Encryption has become a required frontline (or beachhead if you will) for defending your data from exposure. Encrypting data at-rest on devices becomes a key technical control to implement. Encrypting data in-transit, such as when sending a data backup to the cloud or communicating sensitive data, is crucial as well. Make sure data is automatically encrypted rather than relying on the diligence of employees. Encryption is something most organizations should be doing but are not. The fact is, you do not have to break the bank or overcome hard technology challenges to implement successful encryption solutions.

Again, it's vital to constantly educate employees – in digestible snippets – about data security, privacy, policies, and their personal responsibility as data custodians. Ingraining these points into every employee's behaviour is necessary to maintaining effective data and system security while working remotely or from home.

F is for Firewall.

Ensure that employees have a personal (device-based) and a network firewall to help to protect your company's systems and network from any attackers trying to get in.

A WORKSHEET FOR ORGANIZATIONS ENABLING SECURE REMOTE WORK

This non-comprehensive checklist includes a combination of tools, practices, and policies which can be easily adapted to your specific organization. The general disciplines used for a safer distributed work environment (i.e., remote working or work-from-home) form a basis for data and system security best practices that employees should have in place:

- Ensure antivirus, anti-malware and anti-spam solutions are running and updated.
- Ensure and continuously check that the local firewall is ON.
- Maintain an inventory of all devices in the hands of employees. Do this even if these are employee-owned devices used to access company systems/apps, or it potentially stores any data.
- Enforce the use of strong passwords on all devices, even on employee-owned devices (especiallyon non-domain connected standalone/Workgroup computers).
- Enable and properly enforce local encryption on devices, even on employee-owned devices.

- Ensure screen timeouts and screen auto locks to avoid possible exposure.
- Secure any (and all) USB storage devices plugged into any employee-used computer (PC or Mac).
- Maintain a robust data backup plan for all important and work-in-progress data files.
- Enable basic Mobile Device Management (MDM) for remote lock/wipe capabilities.
- Conduct application auditing and remove unwanted and unused apps.
- Enable security policies with tools that can be centrally reviewed and monitored.
- Enable multi-factor authentication (MFA) for remote connectivity and computer access.
- Ensure capabilities are in-place to quarantine data on remote devices when necessary.
- Establish an incident response system and have a simple and unambiguous procedural manual.
- Limit external storing and sharing of sensitive data in personal clouds (OneDrive, Dropbox, etc).
- Ensure remote workers change the default password on their personal WiFi routers.
- Use WPA2 or stronger encryption when setting up WiFi connections, especially personal devices.
- Disallow the use of any public WiFi for work purposes and system access.
- If possible, set up automatic OS and software updates.
- Request that employees lock-up laptops and other business devices when not in use.
- Use a VPN on devices connecting to the organisation's network/systems.
- Train employees to use email with care and encrypt sensitive outgoing company emails.
- Educate employees to be wary and vigilant of phishing attempts and suspicious download links.
- Create and enforce policies around social media postings and other communications.
- Watch out for shadow IT.

BeachheadSecure by DLS Technologies

Using the remotely managed BeachheadSecure platform, DLS easily enforce unobtrusive encryption and data security for all company and employee-owned devices in use within your organization, including for a distributed work computing environment (i.e., remote workers and work-from-home). The BeachheadSecure platform allows DLS to manage the security of all devices from one consolidated administration console. BeachheadSecure provides support for native encryption on PCs (EFS, BitLocker, or both),Macs (FileVault), iOS devices, Android devices, and USB flash drives.

BeachheadSecure as a monthly or annual pay-as-you-go subscription service, with no hardware or software purchases or long-term commitment required. DLS handle every aspect of the solution on your behalf, from deployment to management, monitoring to compliance auditing. BeachheadSecure's cloud-based management means troubleshooting, and remediation is handled remotely, reducing downtime, and maximizing your employee productivity.

The worry and hassle-free BeachheadSecure service is the only monthly pay-as-you-go service that not only encrypts data but can lock out a user or kill device access if this becomes necessary. For those unfortunate scenarios where encryption is not enough – when a password is compromised, when devices with open sessions and credentials entered fall into the wrong hands, when malicious former employees try to access company systems, etc – BeachheadSecure delivers the means to cut off these avenues that would otherwise result in data breaches. The closed-loop communication of BeachheadSecure and its integrated reporting makes it simple to not only monitor but effectively prove your measures for compliance.

BeachheadSecure offers superior data protection, and helps you sleep better at night!

"Part of our decision to select BeachheadSecure for our mobile and workstation data encryption – and to assist us in our compliance strategy – was due to its implementation simplicity and user experience. Other data encryption solutions we looked at were difficult to set up and even harder to manage. We desired a solution that would not interfere with our users and their productivity in any way,but that would still give us the high level of security and audit reporting we require. Beachhead's technology has helped us greatly in our security and compliance efforts."

- Ralph Hopkins, Head of Information Technology, Cliffe Dekker Hofmeyr Inc.

Any questions or comments????

Write to us	info@dlstechno.co.za
Phone us	+27 82 387 1106
WhatsApp Us	+27 82 387 1106
Visit our Web Page	www.dlstechno.co.za

DLS Technologies (Pty) Ltd Feb 2021