Hints and Tips for setting up a Work From Home Facility

The material below has been compiled from multiple sources, and should be used for guidance only.

The coronavirus (COVID-19) outbreak has forced us to remain at home. As companies, we should try to do whatever we can to continue operations in the face of this emergency.

High-profile tech companies such as Google and Microsoft are encouraging or mandating that staff adopt a work-from-home policy. For modern tech companies, the infrastructure and policy needed for remote working are already in place and the vast majority of staff members are probably already laptop users.

For many smaller companies and organizations, however, the situation is likely to be very different. Remote working is probably limited to a few, and realistically mainly for email and other non-operational systems. The education sector is a good case in point: universities have been delivering distance learning as a feature for some time, while high schools and others are mainly dependent on staff and pupils being on-site to learn. The school's operations and administrative teams also need to be considered, as they are unlikely to be mobile workers and may be using desktop devices rather than laptops.

Breaking the organization into just a few groups with differing requirements and dealing with the needs of each to effect the mass exodus may seem a simplistic approach, but is probably essential given the urgency.

In order to be productive, there are common requirements that all remote workers need. The last two are for the employee, but are **fundamentally important**.

- A computer (or phone/tablet)
- A good internet connection
- E-mail, chat and conferencing applications
- Access to documents on-line
- Workflow application
- A dedicated workspace (preferred)
- Optionally, a phone
- Self-motivation and discipline
- A strict routine

Why is the phone optional? In today's environment it may not be necessary, especially as most chat applications allow direct calling. The need for a phone may be a business requirement rather than an essential device.

Importantly, companies and organizations also need to prepare themselves and their employees for the increased **cybersecurity risks** associated with remote working. What are some of the challenges that may need to be addressed?

Physical security of company devices

Employees will be exposing company devices to greater risk as they leave the safety and security of the workplace. Devices need to be protected against loss and theft with options such as:

- Full-disk encryption ensures that even if the device falls into the wrong hands, the company's data is not accessible.
- Log out when not in use – both at home and in public places. An inquisitive child accidentally sending an email to the boss or a customer is easily prevented, as is limiting the opportunity for someone to access the machine while your back is turned in the local coffee shop.
- Strong password policy – enforce passwords on boot, set inactivity timeouts, and ban sticky notes with passwords on them!
- Never leave the device unattended or on public display. If it's in the car, then it should be in the luggage – out of sight.

What's in the home technology environment?

Ask employees to audit their own home environment for vulnerabilities, before connecting work devices. There are continual disclosures regarding vulnerable Internet of Things (IoT) devices, and this is an excellent time for employees to take action on securing them with strong passwords and updating their firmware/software to the latest versions.

Consider promoting, or even mandating, the use of a connected home monitoring app before allowing work devices to be connected to home networks. The scan or monitoring will highlight devices with known vulnerabilities, outdated software or firmware, or default passwords that need to be changed.

Accessing the company network and systems

Establish if the employee needs access to the organization's internal network or just access to cloud-based services and email. And take into consideration whether the same *level of access* to *sensitive data* enjoyed on-site should be granted when the employee is off-site.

If access to the organization's internal network is needed:

- I recommend this is only achieved from an **organization-owned device** so that full control of the connecting device is under the management of the technology security and IT team. However, if employees use their own devices, *Bring your own Device (BYOD)* software should be installed on them.
- Always use a VPN to connect remote workers to the organization's internal network. This prevents man-in-the-middle attacks from remote locations: remember that since you're now working from home, the traffic is now flowing over public networks.
- A *remote desktop* system may be used to prevent applications on the PC to access your systems.
- Control the use of external devices such as USB storage and peripheral devices.

Allowing access to email and cloud services from an employee's own device:

- Enforce the same endpoint security policy for anti-malware, firewalls, etc. as with an organization-managed device. If necessary, furnish the employee with a license for the same solutions used on the organization-owned devices. If you need extra licenses, then contact the provider. They may have solutions to cover you through this unprecedented event.
- Limit the ability to store, download or copy data. A data breach can happen from any device that contains sensitive company data.
- Consider the use of virtual machines to provide access: this keeps the employee in a controlled environment and limits the exposure of the company network to the home environment. This may be more complex to set up, but could be a superior longer-term solution.

- Multifactor authentication (MFA) ensures that access, whether to cloud-based services or full network access, is by authorized users only. Wherever possible, use an app-based system or physical hardware token to generate one-time codes that grant authenticated access. As there may be time pressure to deploy a solution, an app-based solution removes the need to procure and distribute hardware.
- App-based systems provide greater security than SMS messages, especially if the device used to receive the codes is not an organization-managed device and could be subject to a SIM swap attack.

Collaborative tools and authorization processes

It may seem strange to put these two items under the same heading, but one can help prevent issues with the other.

- Provide access to chat, video and conference systems so that employees can communicate with each other. This provides the productivity tools needed and helps employees to remain social with their colleagues.
- Use the collaborative tools to protect against unauthorized instructions or transactions.

Cybercriminals will likely use the opportunity of remotely located workforces to launch Business Email Compromise (BEC) attacks. This is where a bogus urgent demand is sent by a bad actor, asking for the urgent transfer of funds, without the ability to validate the request in person. Be sure to use video conferencing/chat systems as a formal part of the approval system so that validation is made “in person”, even when remote.

Training

As per sources from the internet, there are numerous COVID-19 scams identified, leading to face masks, vaccines, and disinformation. When employees are relocated out of the workplace and placed into the more casual atmosphere of working from home, they may consider clicking on links, as there are no colleagues who might see them watching that amusing video or visiting a webpage.

Cybersecurity awareness is a requirement for employees. It would be prudent to offer a refresher to help avoid the human element that cybercriminals attempt to exploit. Consider running a campaign and training requirement before the employee begins working remotely or as soon as possible thereafter.

Support and Crisis Management

In the rush to provide remote access, don’t sacrifice cybersecurity or the ability to manage systems and devices. The ability to support users remotely will be essential to ensure smooth operations, especially if users become quarantined due to health concerns. Remote workers need to have clear communication protocols for IT support and for crisis management if they encounter unusual or suspect issues that could be the result of a breach.

There are, of course, additional considerations from a technology perspective.

Beyond technology and functional processes, there are other key factors to effective remote working:

- Communication – Consider having team calls once per day, brief people on the status, and give everyone the opportunity to share experiences and issues.

- Responsiveness – Remote working is not the same as working in an office environment. Establish clear guidelines of how quickly a remote worker is expected to respond to a request depending on the communication type, email, Slack, calendar invites, etc.
- Reporting – Line managers need to implement procedures that allow them to ascertain whether the remote workers are getting the job done: mandatory group meetings, team collaboration, daily/weekly/monthly reports.
- Working schedule – Agree a method of clocking on and off, even if it's as simple as a team group chat and members saying good morning when they start their day.
- Health and safety – Do the ergonomic keyboards in the office need to be taken home to provide the same comfort employees are used to? Working from home does not remove the responsibility to provide a good working environment.
- Liability – Ensure coverage for the company assets while in the employee's possession.
- Tech support – Distribute the contact details: all remote workers need to know how to get help when needed.
- Socialization – Bring remote workers together, particularly virtually. Social interaction is an important part of motivation and increases productivity. Consider a buddy or mentor scheme so that every employee is paired and can problem solve, vent, share or socialize virtually.
- Accessibility – Establish a virtual open-door management policy, just as there is in the office. Make sure people are accessible and can be easily engaged.

Don't assume that all employees can switch to remote working effectively and with little assistance or guidance. Home is not the office and they may need significant assistance to adapt.

Philosophically, the world may never be the same again as this mass remote working mandate could prove to be a social/work experiment that few companies would have ever undertaken on such a scale. Will we ever return to our office in the same way?

Stay safe – and healthy!