Remote working

And your cybersecurity considerations during the global pandemic.

Aaron Yates, Chief Executive, Berea
Monday, 13th July 2020

Berea.

The pandemic has changed how our businesses operate. Recent surveys highlight that many feel their quality of life has improved, and we do not wish to return to our prior way of life.

As such, it is likely that remote working will become a key fixture, and key benefit, of how modern businesses are operated.

Anticipating this permanence, now is the time to consider a longer term approach to the changing landscape of how modern business is conducted.

www.berea-group.com

What is remote working?

"Remote working" is the holistic approach, by a business, enabling their people to work from anywhere - at home, a cafe, or even a different country. Ultimately, the goal is that physical location should not matter, as long as work is undertaken correctly and productively.

Facilitating this capability, modern computer hardware is portable, powerful and affordable.

Most clerical tasks can be easily undertaken on a single screen, though extra screen real estate (additional computer monitors) are easily and affordably obtained if beneficial.

To a degree, this can be thought of as akin to "hot-desking", where a workstation is set up, and can be occupied by any individual with a device to plug-in.

In fact, some newer mobile phones and tablets, e.g. Samsung Galaxy running Samsung DeX `https://www.samsung.com/uk/apps/samsung-dex/`, can now be plugged in to a computer monitor to become a functional desktop computer. Rather than assigning a colleague both a laptop and a phone, this concept can present an attractive cost saving.

However, it is very important to understand that "remote working" is not simply the process of providing the technology that enables remote working. It is of critical importance to consider how your business will govern the use of this superpower and ensure operational security.

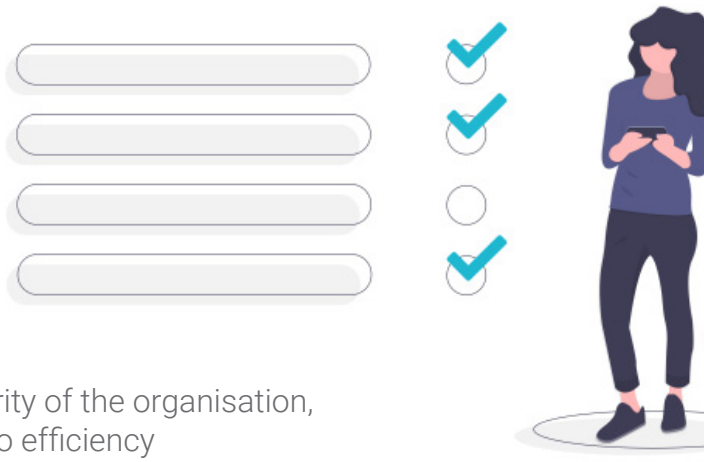
Free, online Cyber Essentials support service
www.cyber-ami.com

Governance of remote working

Governance is typically implemented through HR policy, managed through defined processes, and explained to colleagues through training. Little knowledge of a topic matter can make implementation of such a regime a hard-fought battle.

Fundamentally, parameters must be established that meet the needs of the business, and their importance explained to the end user.

Otherwise, the regime may be merely ignored, entirely overlooked or consciously circumvented, leading to failure of the strategy.



A remote working governance regime will focus on security of the organisation, including legal and contractual compliance, and further to efficiency and productivity in wider business operations. The regime needs to be manageable, measurable and consistently applied.

Governance often starts with the question: what can go (or has gone) wrong, and how do we reduce the likelihood of that issue in the future?

To this end, we need to understand some of the issues that remote working can present.

Free, online Cyber Essentials support service
www.cyber-ami.com

What can go wrong?

Let's consider some common scenarios, and how they might influence our thinking on governance of remote working.

A quick note:
This list is by no means exhaustive; all eventualities must be considered and prepared for. Pre-agreed (and understood) recovery plans for each are essential.

Computer hardware can fail, and computer devices can be lost, misplaced or stolen.

- In the event of device failure, theft, or loss, your colleague will be unable to operate within their team.
- In the event of theft or loss, sensitive data stored on the device can be considered as being exposed to unauthorised individuals - i.e., a data breach.

Cloud services can fail, be discontinued, or suffer incidents of their own.

- If you are dependent on these tools for 'business as usual', your entire operations may grind to a halt.
- Should the service suffer it's own cyber incident, data may be exposed to unauthorised individuals. In the worst case, it may be lost entirely.

Internet connections can be disrupted.

- Home users are unlikely to have "business level" service level agreements. If their home broadband has a 99% uptime guarantee, an individual can still lose their connection for almost 90 hours in a year (equating to over 10 working days), preventing them from working.

Computers are used by people, who are not infallible.

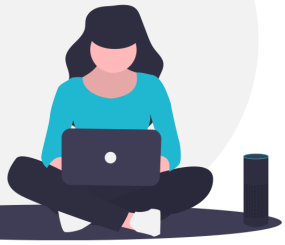
- The best approach to security is in layers. Technical controls, policy, process and training can only go so far. Our first (and best) line of defence will always be a computer user who is actively and consciously engaged with security in their day-to-day routine.
- Remote working can instill a very different mindset than that used in an office. With inexperience of the working practice, combined with no immediate oversight, and no chance of micro-interactions with colleagues, simple queries might not be asked, and concerns might not be raised. This creates fertile ground for social engineering attacks.
- Should a colleague's personal device suffer misfortune, they may be inclined to use a work device for personal purposes. After all, who will ever know? This situation can leave the work device exposed to wider malware threats from dubious websites.

A strategy for the longer term

An effective remote working governance regime will consist of policy, process and training. These should be regularly assessed and reviewed. As a starter for ten, some initial considerations may include:

On-boarding of new colleagues

Setup and configuration of a new device to approved specifications. This should, at a minimum, include a defined (password protected) user account without administrator privileges, antimalware software, software updates set to automatic where possible, and the provision for on-site and remote incremental backups.



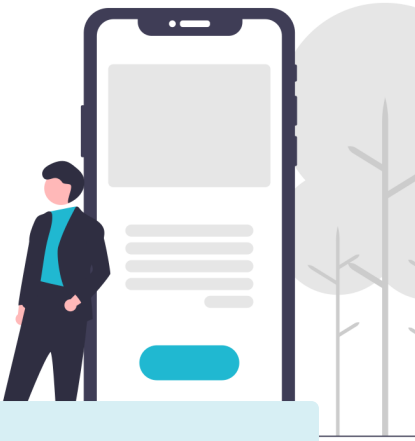
Before being permitted access to a company owned device, service or data, individuals must receive role-appropriate training on information security and data protection practices.

New colleagues should be required to read and accept your policies pertaining to these subjects. They should feel confident in being able to ask for help or advice should they have any concern over security or use of their device.

Day-to-day work

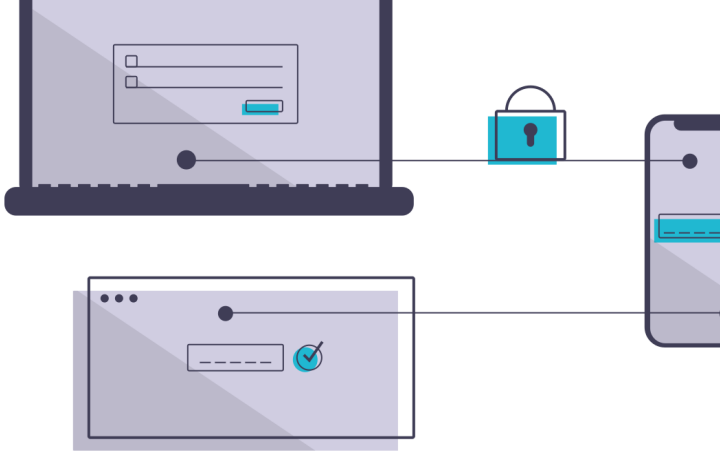
It is of utmost importance to consider the security of the home or place of remote work. Devices that can access sensitive systems or data should be stored securely when not in use. They should not be used for personal purposes, by the colleague or their family or friends. Consideration should be given when working in a public place that sensitive data cannot be seen on the screen by others.

There is, of course, a health and safety consideration in remote working. Most offices are designed to be ergonomic, to reduce the likelihood of repetitive strain injury. Many homes do not possess a dedicated workstation or office chair. We are aware of some instances where ironing boards have been used as a makeshift desk.



Prolonged use of such a setup may cause injury, preventing the colleague from working. A health and safety risk assessment should be undertaken, and regularly reviewed, to ensure an optimal working environment.

Free, online Cyber Essentials support service
www.cyber-ami.com

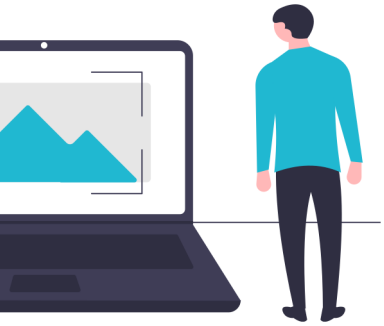


Off-boarding of leavers

Your colleague exit process should include differe
security procedures for “good” and “bad” leavers.
Usually, the only difference will be the time that th
ability to access services, accounts, or other sensi
data stores is rescinded.

I.e. a bad leaver will have service access rescinded immediately, where a good leaver may work their notice period.

You may or may not be able to undertake a successful handover. This should inform your thinking of induction, in that, where possible, that individuals should maintain documentation of work undertaken in their role.



You will want to safely recapture any assigned hardware. You should maintain a process for accounts and services to be disabled and licences or retained data redistributed accordingly within the business.

Older computer hardware may not be able to receive modern operating system updates, so this may be an ideal time to securely dispose of the device.

Free, online Cyber Essentials support service
www.cyber-ami.com

Confidence and assurance

Defining a security regime for a business can be complex. Rather than recreating the wheel, many look to established assurance specifications to benchmark themselves against.

Adherence to these frameworks can provide confidence within the business, and, importantly, to customers and prospects.

Your starting point should be HM Government's Cyber Essentials scheme. This is considered the minimum benchmark of information security practices for all British businesses. Following the requirements can reduce exposure to common threats from the internet by up to 80%, and an official certificate of compliance can be obtained.

A free-to-use, online service exists that can help you understand and implement Cyber Essentials. You can obtain your certificate, if desired, for a fee at the end of the process.

You can register and get started in under a minute, and there's nothing to download. Learn more and get started here: **https://www.cyber-ami.com**

Free, online Cyber Essentials support service
www.cyber-ami.com

Berea.