Remote working and security considerations

Remote working is a long-lasting effect of the pandemic, but it raises potential cyber security issues, says Simon Bulleyment

"RISKS THAT IN THE PAST HAD BEEN (MOSTLY) UNDERSTOOD, MITIGATED, AND WELL-MANAGED, SUDDENLY CHANGED AND NEW ISSUES AROSE"

Simon Bulleyment
is a director of Sibrossa

CAST YOUR mind back to January 2020, and you will recall the media started to talk about a new type of coronavirus, and people falling ill with something called Covid-19. As the weeks ticked by, the urgency of the situation grew and charities started to plan for something called "lockdown", and work out how on earth they would continue to operate with most/all of their workforce based at home.

What took place in a short period of time was arguably the largest amount of IT change ever seen. In the rush to get remote access systems upgraded or deployed in early 2020, unfortunately security often took a back seat.

Three years on, remote working is here to stay and remote access/videoconferencing systems are critical IT components for most charities. In general, remote access systems generally fall into the following three categories:

- **Remote desktop** – where IT processing, such as running applications, accessing Microsoft Office/files etc takes places on a back-end server. Screen, mouse and keyboard data is transferred between it and end-user laptops/PCs.
- **VPN** – where IT processing takes place on laptops/PCs and data is transferred securely across the internet between them and back-end server resources, establishing a virtual private network.
- **Cloud-based apps and systems storing business data** – laptops, smartphones etc connect to a website or app and data can be accessed or transferred to devices.

REMOTE ACCESS SYSTEMS

In general, there tends to be fewer risks with remote desktop systems as data usually stays on back-end servers. However, user experience can be an issue and charities may therefore favour the use of VPN systems.

> "Unfortunately security often took a backseat"

Historically, IT systems generally comprised of internal networks and a perimeter firewall between them and the internet. IT teams would implement controls to defend the perimeter against internet-based attackers and they would also have solutions in place for the ongoing management of end-user devices. Fast forward to the Covid pandemic, and this model was broken. End-user devices were frequently only connected via the internet, rather than in an office, making device management complex, and effectively distributing network perimeters to wherever staff used their laptops and tablets. Risks that in the past had been (mostly) understood, mitigated, and well-managed, suddenly changed, and new issues arose, including:

- Vulnerabilities because of rushing to implement remote access systems. These included weak authentication controls for establishing remote access (end-users can be relied upon to choose poor passwords).
- Lack of device visibility and ongoing management, for example being able to install security updates to mitigate risks from attackers exploiting software vulnerabilities.
- With home working, the internet perimeter effectively moves to broadband routers. IT teams almost never have management capabilities over them and therefore cannot place reliance on their technical controls. Consequently, perimeter-type technical controls had to be replicated on each and every end-user device and this was often poorly managed, or not done at all.
- Attackers were only too aware of changes to working practices and began exploiting weaknesses with targeted phishing campaigns.
- Lack of proactive monitoring of IT systems for security events. Many IT departments were swamped with end-user support issues, requests for hardware/peripherals, and dealing with staff who were unable to work. Consequently, security alerts were missed that in the past might have been picked up.

KEEPING SECURE

Given that we are now almost three years on from the pandemic, the situation above will have improved for most charities. However, which controls are necessary to adequately secure remote access systems? While there are many "buzz terms" in the cyber security world, these can be broken down to cover three areas: people, processes, and technology. For the sake of this article, the first two will be swapped around, dealing with the process point first.

A key document for charities to have in place is a remote access policy, covering the remote access systems that are supported, and when and how they can be used. The first decision to make is whether personal as well as organisation-provided laptops, tablets and smartphones can be used. Management and IT teams should bear in mind that irrespective of device types being used, security risks should be assessed and relevant technical controls applied. For personal devices able to access charity data/systems, if controls cannot be implemented to secure them (eg enforcing passwords, ensuring that firewalls are enabled, regularly applying software/anti-malware updates etc) quite simply, their use should be prohibited. Remote access policies should also cover use/storage of charity data. For example, where should documents be stored and, if permitted to save them to end-user devices, what back-up and encryption controls are in place to prevent data loss/theft? This is an especially important point when charities permit smartphones to synchronise (and therefore store) email data.

Once a policy has been created, it should be approved by senior management and updated annually to ensure it reflects changes and updates to the IT environment. It should also be communicated to staff, and this neatly leads on to the next area: people. As this article is not trying to cover hiring processes or selecting the best staff, it will instead focus on training.

Cyber security training should be a regularly recurring process. For remote access systems, it would be wise for training to cover secure use of them. This is also an opportune time to include other relevant policies, such as those relating to data protection/UK GDPR. From a cyber security perspective, the following approaches, or a combination of them, are recommended:

- **Training for new staff.** This can be a webinar-type approach but more effective is instructor-led, perhaps on a quarterly basis to include new starters within that period.
- **Recurring training based on bite-sized, topical content throughout the year.** Many vendors produce systems that automatically send out short videos to staff on a regular basis, covering specific security topics (eg remote access, passwords, wifi etc). This approach has the advantage of not over-burdening staff.
- **Annual/refresher training.** This is best approached as instructor-led and is useful for updating staff on security topics, changes to IT/security systems and updates to policies.

In terms of training for remote working, it is vital that common cyber threats, such as phishing and ransomware, are included. This should cover how attacks work, how staff can spot them and best practices for avoiding being duped into doing something they should not do. Training content should be updated regularly to address the constantly evolving nature of cyber attacks.

> “It is vital that end user devices are kept secure and up to date”

The National Cyber Security Centre (NCSC) provides some very useful (and free) training for charities (https://bit.ly/3CQLHXK).

The final area for this article is technology, or specifically key technical controls that should be in place to secure remote access systems. Ultimately charities should select these based on their own risk assessments; however, the following will likely feature for most IT systems.

Authentication controls are vital for ensuring that only authorised staff gain access. There are many approaches that can be taken but the simplest is to allow staff to use their network password, ie a single username and password to access the network both in the office and while working remotely (referred to as single sign-on or SSO). However, passwords alone should not be relied on as staff can (and will) set them to be insecure or use the same details to access other systems and websites. Attackers are aware of this and when they gain access to password databases, they will try and use credentials for logging into other systems. A very effective control is to use multi-factor authentication (MFA or sometimes referred to as two-factor authentication, 2FA). This significantly enhances log-on security by requiring a password and something else, often a pseudo-random code generated by a smartphone app.

If your charity is using a VPN, it is vital that end-user devices are kept secure and up to date to ensure that any threats on them, such as malware, cannot travel across the internet and attack data on back-end systems. Main areas to consider are ensuring anti-malware systems are kept updated, regularly installing software updates and ensuring firewalls are enabled and are controlled centrally. Furthermore, devices should be regularly monitored for security vulnerabilities.

ENSURING REMOTE ACCESS SYSTEMS ARE SECURE

Having addressed policy, training, and some key technical controls, how can management ensure that remote access systems have been securely implemented and are being managed effectively? One answer is to consider the government-backed Cyber Essentials (CE) and Cyber Essentials Plus (CE+) schemes. These are frameworks that, if implemented properly, aim to protect any size of organisation from the most common form of cyber-attacks.

NCSC provides guidance at https://bit.ly/3XfUwCO.

NCSC has also recently launched the Funded Cyber Essentials Programme, which provides eligible charities and organisations with around 20 hours of free consultancy time. Further details can be found at https://bit.ly/3XyuSsF.

Cyber Essentials consists of a questionnaire covering a detailed set of security controls. Those responsible for IT complete it and the CEO, or equivalent, authorises it. Questions are marked by an external assessor, who may seek evidence to support responses. CE+ takes this one stage further, by bringing an external assessor onsite to perform tests that ensure controls have been implemented and are working properly. Finally, an alternative is to consider an external cyber security audit. This can provide an independent assessment of security controls across a wide range of areas, leading to a report identifying risks and recommendations for improvement. ●