EBOOK SERIES

Just how **secure** is your **remote workforce**?

Professional cyber security advice and practical solutions to help protect remote and hybrid workforces.

infinity group

Contents

Introduction

"The percentage of businesses deploying security monitoring reduced from 40% to 35% in 2020. And reduced again in 2021."

Navigating the ever-evolving digital terrain to facilitate remote working, has been at the forefront of the operations of many businesses around the globe, since the pandemic began. Organisations were forced to move their entire workforces into remote working setups quickly.

Two years in, and remote/hybrid systems are now commonplace. However, for businesses it's now time to take a step back and consider the cyber security implications of your remote working setups. Although a crucial subject, it has been moved down the priority list of most companies.

The frequency of cyber security attacks has increased by 62% since the beginning of the pandemic[1]. Business have fallen victim to cyber-crimes such as phishing, hacking, identity theft, fraud and malware. This has led to increasing conversations about the risk around Cyber Security and how to mitigate it. The UK Government's Cyber Security Survey also revealed that the percentage of businesses deploying security monitoring reduced from 40% to 35% in 2020[2]. And reduced again in 2021.

In this eBook, we have highlighted the issues surrounding cyber security for businesses with remote and hybrid workforce practices and the types of measures that should be considered to ensure full protection going forward.

References

[1] *2020 IT Governance Blog*

[2] *UK Government Statistics 2021*

1 What is Cyber Security?

Now businesses are setup to work remotely, it's time to consider the cyber security implementations of remote workforces.

Cyber security is the implementation of processes and controls to protect systems, networks, hardware, software, data and devices from online cyber threats. Cyber attacks involve data theft, unlawful data access, sensitive data being leaked and compromised networks. Cyber security threats come in many different forms, some examples include phishing, malware, ransomware, password attacks, network breaches and insecure Wi-Fi access.

Businesses that fall victim to cyber-attacks experience significant losses to data and disruptions to networks and IT infrastructure. As a result of this, cyber security is a practice that should be taken seriously.

The importance of a Cyber Security Approach

The Covid-19 pandemic led to the rise in remote working for employees globally. With most businesses now choosing to work remotely or in a hybrid setup on a permanent basis, cyber security concerns have noticeably become more prevalent.

Post Pandemic Security Risks

In the rush of 2020, where businesses tried to get their employees to work remotely over a short period of time, the focus was on making sure they were set up remotely to continue their daily duties. Some businesses did not consider the additional cyber security risks posed by this new arrangement and failed to foresee the cyber security implications; others have meant to revisit it but have not yet done so.

2 Personal Device Security Breaches

Businesses now need to assess these risks and understand the threats personal devices pose.

Pre-pandemic, many businesses had suites of desktop PCs that were office based and these were then replaced by laptops or their own personal devices that were then used for work purposes. In other instances, applications could only be accessed from the office space when close to a server and these have now been moved to the cloud.

IT teams across the globe, as well as our Service Desk had the task of setting up thousands of employees with VPN Desk access (Virtual Private Networks) to enable them access to certain applications and data from their own personal or brand-new company devices. However, when personal devices are used for work purposes it is very hard to manage what levels of security protection are enabled e.g. Devices without anti-malware applications installed could potentially cause breaches.

In addition, we have witnessed that the control and process management of regular password updates and the enforcement of secure passwords for remote workforces have relaxed overtime. When cyber security training is not a priority for businesses, the risk of devices becoming intercepted and compromised is inevitable.
Moving forward, and as a preventative measure, businesses need to assess these risks and understand the threats personal devices pose. We recommend that accessing VPNs from personal devices should also be avoided as they can act as an easy target for ransomware attacks, leaks, and malware. Confidential data should be encrypted to avoid GDPR compliance issues.

3 Shadow IT Threats

"Employees need to be encouraged to be transparent about the software they currently use."

Post pandemic remote working has also increased the levels of Shadow IT. Remote workers commonly use applications and software not previously approved by their respective IT departments to help with team collaboration, screen-sharing and messaging. These are often installed by employees with the notion that they help them work more effectively, but without any consideration or knowledge around the security threats that these applications could pose.

This has led to increased challenges for IT security, in the form of sensitive data losses and leaks, financial risks and compliance issues, among others.

To combat this, our Cyber Security team recommend businesses consider implementing a regular audit of third-party applications in use by employees. To do this audit well, employees need to be encouraged to be transparent about the software they currently use. And, once this has been completed, risky applications need removing and a list of banned ones should be publicised to employees with corresponding risks outlined.

In addition to the findings, a deeper analysis needs to be done into common trends. What is the common theme of these applications? This will determine the functions that the approved business applications are not providing the employees at present. At this stage, your team can then investigate which secure cloud solutions would work for everyone across the business.

4 | Rise of Shadow IT

"1 in 5 organisations have suffered a cyber attack as a direct result of Shadow IT."

There has been a sharp increase in the use of shadow IT. Check out some of the statistics:

59% increase in shadow IT use since the beginning of the COVID-19 pandemic.

35% of employees admit they have had to work around security policies to get their work done.

67% of teams have introduced their own collaboration tools.

83% of IT professionals reported that users have been known to store company data in unapproved cloud services.

1 in 5 organisations have suffered a cyber-attack as a direct result of shadow IT use.

So, what are the users turning to?

- Messaging apps like WhatsApp or Snapchat
- Cloud storage such as Dropbox, Google Drive, personal Microsoft OneDrive accounts
- Personal communication apps – Teams, Skype, VOIP platforms
- Productivity tools like Slack or Trello

The focus therefore needs to be on giving users the tools they require, coupled with the freedom and flexibility they need to work, for maximum productivity. That means adopting the principles of the modern perimeter as discussed in an earlier blog, adopting IT management and security frameworks and keeping a finger on the pulse of users through training and feedback.

9 | Threats from Insiders

"Time to take action. The 'Great Resignation' poses a huge threat for insiders to leak data before they move to their next role."

Insider risk occurs when former employees, contractors, or third-party vendors with insider information about cybersecurity practices, leak data out of the business. The categories can be classified into those with the intention of leaking and those who leak data unknowingly through their negligent work habits.

There has been a huge surge in insider risk throughout the pandemic and this continues to grow as a result of the 'Great Resignation' as insiders working remotely have access to sensitive large files.
IT teams within businesses need to constantly monitor files and activity across key data sources and most importantly, ought to implement applications to identify and determine who has access to data so as to prevent these types of threats.

Protection of data at a deep level, beyond a traditional permissions structure, offers that level of safety from any device globally, by providing security to the documents themselves. That protection will travel with it, wherever it goes.

10 The Modern Security Perimeter

> *Form a flexible perimeter that surrounds your business regardless of where users are, or what they're doing.*

Before remote working, the edge of an organisation's network, or rather its firewalls, were considered the perimeter and everything that occurred within the security perimeter was trusted.
In a world of flexible, remote or home working as the norm, coupled with modern threats like ransomware, phishing and social engineering, that definition of the perimeter is no longer true. Most businesses now also have some form of cloud presence, whether that's Microsoft 365, Google, or cloud applications, they all sit outside of your fort, and have big targets painted on them. Businesses that still rely on the legacy perimeter are in this situation.

Implementing a modern security perimeter
The modern perimeter acts as a series of boundaries in a decentralised IT world that aims to protect data and identities in a workplace from anywhere world.

These three important pillars form part of a modern perimeter:

- Identity
- Devices
- Data

Each element protects the business in a specific way, but all the pillars collectively form a new, flexible perimeter that surrounds your business regardless of where users are, or what they're doing.

11 The Three Perimeter Pillars

1. The Identity Pillar – Businesses need to have a centrally managed identity management platform that controls access to all their resources, wherever they are, or from whatever device they're accessed from. That needs to apply regardless of the device – Windows, Mac, mobile – company or personally owned.

They should also be challenged with Multi-Factor Authentication (MFA) when appropriate, ensuring almost without a doubt that they are who they claim. The behaviours of those accounts then need to be monitored to understand what's 'normal' for them, much like banks track spending behaviours. Where do the users typically work from and when? What's usual, unusual and impossible? This helps to build a picture of the risk associated to each sign-in, and block it when it's high, even if the user passed through MFA successfully. Never trust, always verify.

2. The Device Pillar – Today, employees have high expectations when it comes to devices. They tend to want sophisticated devices such as Apple vs Windows or may just bring their own device to work. These devices are then taken to a wide range of places and connected to the internet in a variety of ways.

Users might only be inside the network perimeter for 8-16 hours per week, out of 167. For the remaining 150 hours or so, unless the device is secure, it is susceptible to a plethora of cyber incidents. Multiply that by a large estate of devices, perhaps as many as 2-3 per-employee and suddenly the perimeter is a sieve. And that sieve is full of company data.

"The identity, device and data pillar help define your approach and protect your business."

Businesses need the ability to prevent devices that aren't appropriately secured from accessing their data, whether inside the perimeter or out. If someone brings a personal machine into the office and plugs it into the network, it's another loophole. These devices need to be denied access until they meet a defined set of criteria.
The essentials are:

- Encrypted storage
- Software up to date
- Anti-malware up to date
- Strong password
- Firewall enabled

Additional measures involve centrally controlling all devices via an endpoint management platform. Removable storage should also be encrypted and scanned before use or must be blocked completely.
It is important to note however that too many heavy-handed barriers will encourage users to look for workarounds which may then cause further disruptions. Although security needs to be robust, IT admins need to ensure that they are not obstructive, within modern workplaces setups that exist today.

3. Data – Data needs to be protected at the document level across the cloud. Users between which files are shared should be carefully monitored by IT personnel.

The aim is to prevent both deliberate and accidental data leakage or theft, whilst avoiding any need to implement those obstructive barriers that could tempt people to seek workarounds.

Overall, the highlight to take away is that just because it's happening inside your office or on one of your devices, that doesn't mean it's safe or secure.

12 | Cyber Security Measures

"The Cyber Essentials certifications demonstrate your commitment to cyber security and also enable you to participate in bigger tender opportunities"

Cyber Essentials Certifications

This is a UK government-backed scheme which is aimed at providing guidelines that organisations need to follow to affirm their commitment to cyber security. Having this cyber security framework is beneficial to the operations of your organisation. It is also supported by the National Cyber Security Centre (NCSC).

The demand for Cyber Essentials certifications has increased over the past 18 months as businesses look to improve their cyber security stance. The use of third-party tools such as videoconferencing, multimedia apps and task management tools are continually on the rise as employees look for new ways to boost their efficiency and especially within those businesses who have adopted a permanent remote working approach.

The Cyber Essentials program helps organisations to mitigate against phishing attacks including malware, malicious emails, website links and hacking opportunities by exploring the known vulnerabilities in internet connected servers and devices.

13 Cyber Essentials Certifications

Cyber Essentials Standard – This affordable certification is awarded based on a declarative self-assessment. However, to achieve this, the business needs to put in place a series of detailed policies and processes which take time to assess and implement. Infinity Group can help businesses to focus their efforts on implementing relevant and right-sized solutions.

Once achieved we can advise on completing the assessment via the online questionnaire. This completed assessment is then submitted to IASME for marking by a certified assessor. If the submission is successful, Cyber Essentials Standard is awarded as a result. If the submission is not successful, one of our certified assessors, can assist in a quick turnaround for remedial works and re-submission.

Ideal for businesses who:

- Want to demonstrate Government backed IT Security compliance
- Are looking to enhance their IT security
- Are interested in gaining the included Cyber Liability cover
- Keen to work towards obtaining Cyber Essentials Plus

Cyber Essentials Plus – The Cyber Essentials Plus certification can only be obtained by a business after the Cyber Essentials Standard has been awarded. This certification is awarded by an external Certification Body and offers a higher level of assurance through the external testing of the business' cyber security approach.

Ideal for businesses who:

- Want to tender for large value projects

14 | Cyber Security Frameworks

If you are a Financial Services business looking to advance your cybersecurity, CIS and NIST are our recommended frameworks.

CIS (Centre for Internet Security) – The CIS Critical Security Controls framework encompasses all the elements of Cyber Essentials plus a prescriptive, prioritised set of cybersecurity best practices and defensive actions that can help prevent the most pervasive and dangerous attacks, and support compliance in a multi-framework era. These actionable best practices for cyber defence are formulated by a group of IT experts using the information gathered from actual attacks and their effective defences. The CIS Controls provide specific guidance and a clear pathway for organisations to achieve the goals and objectives described by multiple legal, regulatory, and policy frameworks.

NIST For Financial Services – This framework is developed by the National Institute of Standards and Technology (NIST) to guide private sector organisations to improve the cyber security methods they already employ.

According to the SEC's Office of Compliance Inspections and Examinations (OCIE), about 88 % of Broker-Dealers (BDs) and 74 % of the Registered Investment Advisors (RIAs) have experienced some form of direct or indirect cyber-attacks recently. These statistics reveal the importance of a regulated framework for financial services.

With advancements in the sector such as the emergence of fintechs and mobile applications, regulations and policies are constantly changing. Therefore, IT leaders in financial businesses ought to utilise NIST standards to shield themselves from online invasions.

15 Zero Trust Networks

"The best approach is to assume no employee can be fully trusted with company data."

This process involves putting in place measures to prevent any user from gaining immediate access to a network. This means that there is no 'default trust' from internal or external individuals. This in turn leads to an added layer of security for the prevention of data breaches.

Employing a zero-trust mindset means that organisations should not automatically trust anything inside or outside of their perimeters. There should be thorough verifications done before access is granted to employee downloads. This also includes applications, processes and third-party partners/clients networks and systems.

16 Mobile Device Management MDM

Typically, MDM would be used to manage corporate devices whether they are workstations or mobile devices. They also allow an organisation to manage everything from securing devices and data to managing how devices are updated and what software is deployed for the end user.

Examples of how a device may be managed by MDM:

- System update policies including feature updates to Windows 11
- Disk encryption – BitLocker on Windows and FileVault on macOS
- Set PIN and password requirements
- Configure Wi-Fi and VPN connections
- Deploy security baselines
- Configure apps to automatically deploy based on user /groups.
- Provide a store and whitelisted apps that can be additionally installed based on user needs.
- Easily reset or refresh devices to repurposes devices, or to lock devices that have been lost.
- Autopilot - allow devices to be sent directly from suppliers and allow users to have a seamless out of box experience with all the apps and settings required without needing assistance from IT support.

Since MDM provides a system that can control every element of a device it is usually not warranted on personal devices as this could feel intrusive. But companies still need to ensure their data is being handled securely and that information can be wiped should an incident occur.

17 Mobile Application Management MAM

MAM allows organisations to set policies on a more granular level by addressing the application only and ignoring the device state entirely.

With MAM we can secure the application and the data held within. The advantage of this system is that the end user's device remains entirely separate from the organisation whilst allowing company data to remain secure.

Examples of how applications can be managed by MAM:

- App configuration.
- Isolate organisational data from personal data.
- Secure managed apps with app specific password.
- Prevent copying of organisational data to personal apps.
- Prevent saving and printing of organisational data.

18 Microsoft Enterprise Mobility + Security

Businesses with BYOD policies should have a cloud based management tool in place to ensure they remain in control of what data is being accessed from what location and by who.

It is pertinent to always protect your business devices. The Microsoft Enterprise Mobility and Security (EMS) platform ensures that your business's sensitive information is kept secure regardless of location or device. This promotes an effective BYOD Device Management which should form a larger part of your Cyber Security framework.

As an identity-driven set of Cloud-based BYOD management tools, EMS secures sensitive company documents. This means your business documents can be securely accessed by users regardless of location or what device they are using. EMS can be installed across your wider IT systems, making it easy to manage device security across desktops, laptops, mobiles and tablets.

19 Become ISO 27001 Certified

The ISO 27001 (Information Security Management) is an internationally recognised standard that supports businesses who wish to maintain the highest levels of information security.

It is the only auditable international standard that defines the requirements of an information security management system (ISMS). An ISMS is a set of policies, procedures, processes and systems that manage information risks, such as cyber attacks, hacks, data leaks or theft.

Many businesses looking to work towards ISO 27001 complete the Cyber Essentials certifications first or in line with this accreditation as there is some overlap. Both demonstrate a businesses commitment to cyber security best practise and are a requirement to work with many organisations particularly mid-market and enterprises.

20 Concluding Thoughts

Hopefully the content of this eBook has generated some thought provoking questions around your current cyber security setup and given you useful insight of the types of measures and tools you can implement across your business to strengthen your cyber security approach.

Infinity Group are a top Microsoft Gold partner in the UK who provide specialist cyber security services including security hardening solutions designed to accomodate the needs of remote and hybrid workforces. We have a dedicated Security Operations Centre within our business who provide 24/7 monitoring of networks and devices to identify and block a much wider range of threats than traditional anti-malware solutions would detect.

To find out more about our wide range of Cyber Security services please call to speak directly with a Consultant 0330 191 9900

www.infinitygroup.co.uk

Further Reading

Read our other blogs to find out more about the cyber security implications of hybrid and remote working.

Cyber Security tactics in a Post-Pandemic world

The Top Cyber Security Frameworks

Why is Cyber Security Important?

The Components of a Cyber Security Framework

5 Tips to Improve Cybersecurity for Your Business in 2021

Modern Workplace Security – A Three Pillared Approach

infinity group