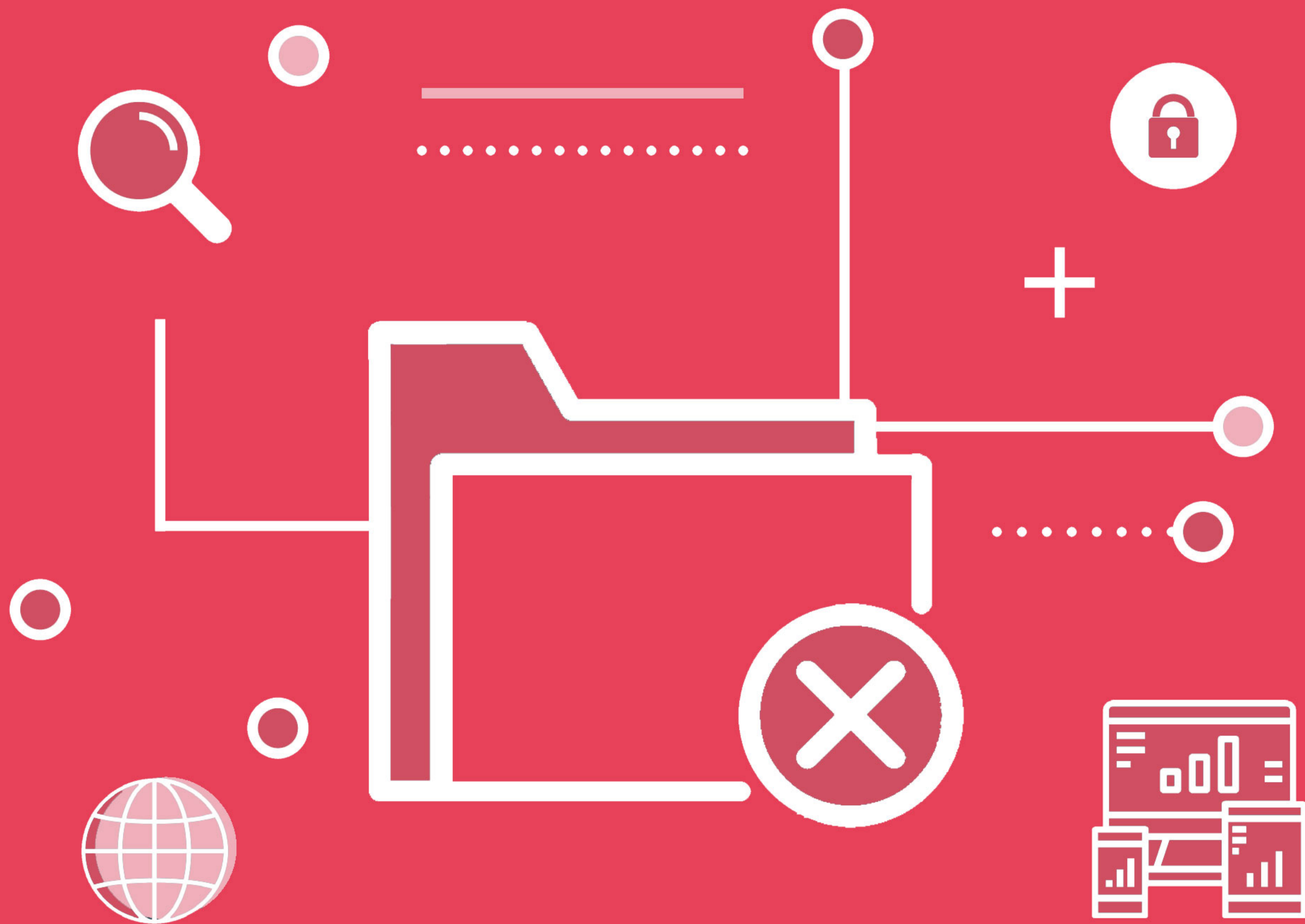


The Bigger Picture

Privacy and Work in the New Normal



Published 22nd March 2021

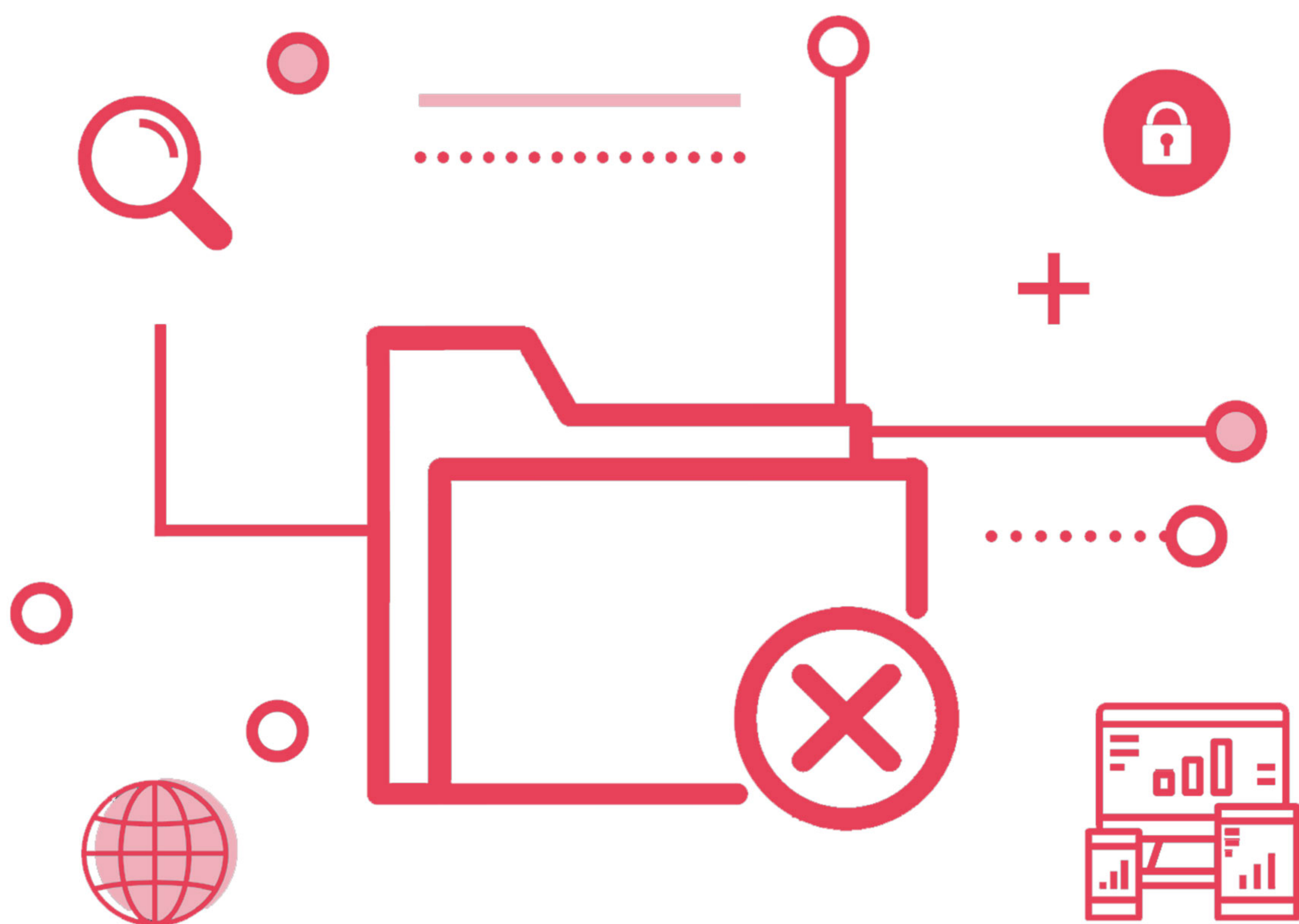
CONTENTS

01 INTRODUCTION

02 MARKET DYNAMICS:

Changing Attitudes & the future of work

03 ROAD TO RECOVERY & THE OFFICE
OF THE FUTURE



01 INTRODUCTION

Prior to the coronavirus outbreak, home working whilst not unheard of, was still relatively uncommon, or in many cases limited to a few days per month. The pandemic, and the resulting lockdown restrictions, have driven a vast segment of the population, particularly in western markets, into remote working. Coupled with government intervention, such as the furlough scheme in the UK, there has been a substantial change in levels of employment over the course of the pandemic, as well as working hours. Likewise, the question of how long the 'new normal' will prevail is paramount: remote working raises numerous concerns around privacy, employee welfare, and productivity; issues which will be discussed further in this research.

1.1 IMPACT OF CORONA VIRUS SO FAR

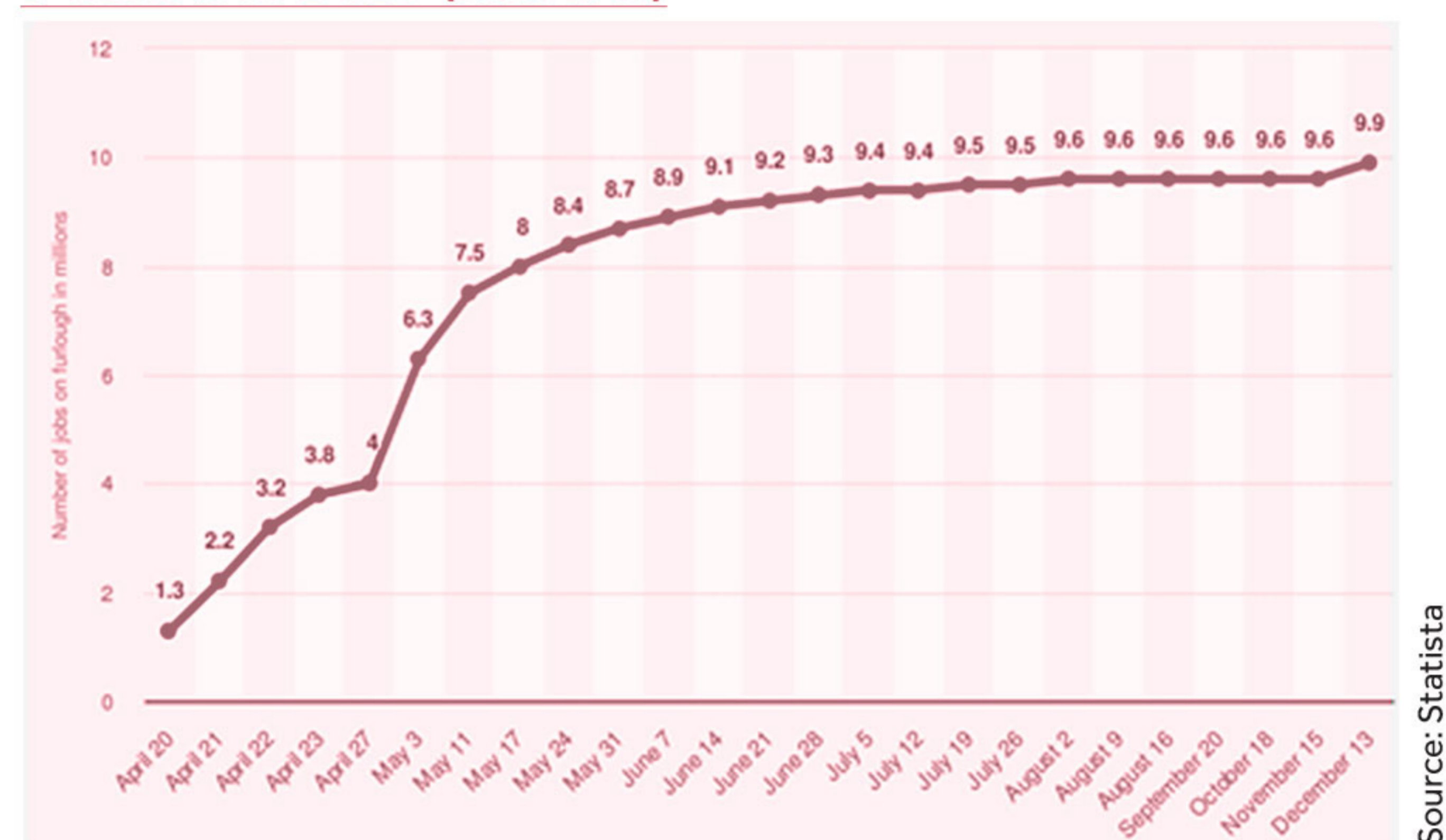
In terms of the scale of the coronavirus impact on business, we have seen significant levels of unemployment even with intervention by the state. Similarly, the cycles of lockdown events, where individuals have been instructed to work from home during the harshest restrictions, have not necessarily led to a full return to offices upon the subsequent lifting of restrictions, thus suggesting a much longer-term behaviour change.

i. Impact on business & employment in the UK & US

The UK has seen not just a hit to personal finances, but also a raft of spending and incentives (such as the furlough scheme) made by government to try to ease the impact on individuals and business. However, even with these in place the unfortunate truth is that there has, and will increasingly be, a significant negative impact on employment rates and business insolvencies, especially as we come to the end of the furlough scheme (presently set for end September 2021).

The UK has seen not just a hit to personal finances, but also a raft of spending and incentives (such as the furlough scheme) made by government to try to ease the impact on individuals and business. However, even with these in place the unfortunate truth is that there has, and will increasingly be, a significant negative impact on employment rates and business insolvencies, especially as we come to the end of the furlough scheme (presently set for end September 2021).

Figure 1: Cumulative number of jobs furloughed under the UK job retention scheme between 20th April and 13th December 2020 (millions)



Source: Statista

According to a recent Bank of England survey: "The impact on employment was expected to be -7% in 2021 Q1 and -5% in 2021 Q2, compared to -8% in 2020 Q4. Employment expectations in the December survey were more pessimistic than in November." It is worth noting that .

December for South East England, as well as the subsequent full national lockdown introduced 6th January 2021. The research also found that the percentage of employees on furlough decreased to 8% in December, down from 11% in November (which followed the end of the second lockdown). In the UK, total hours worked have also fallen considerably. The sectors most affected were those where a relatively high proportion of consumer spending involves face-to-face contact and/or social activity (for example accommodation, and food or recreational services) and those that were most affected by government restrictions (e.g. transport).

The US also saw a dramatic impact on employment figures, with unemployment reaching 14.7% in April 2020, the highest since the Great Depression, and up substantially on the 3.5% recorded two months earlier. By December 2020, unemployment figures had recovered to 6.7%, however given rising cases early in 2021, there will be increasing pressure on this recovery. The US has also suffered from a disjointed approach to coronavirus response. Many restrictions which are in place were decided on a state level, following advice from federal government. This led to 32 of 50 states imposing lockdown by the end of March 2020. Varying strength of restrictions have then continued for subsequent months, often on a state-by-state basis, but sometimes even differing by county.



MARKET DYNAMICS:
**Changing Attitudes &
the Future of Work**

In the following chapter, we explore some of the challenges and privacy concerns this has introduced, as well as looking at how the future of work may look, as the pandemic begins to ease over the coming year. As such, we will assess the 'road to recovery' analysing the return to offices, and whether this will ever be truly achieved. We will also explore how the future of work may look, coupled with threats and solutions for data protection in this 'new normal'. (2021).

i. The rise of remote working

Following the recommendation or requirement by many governments for swathes of the population to remain home during stringent lockdown events, millions of workers across the globe have suddenly found themselves working remotely for sustained periods since spring, 2020. It is estimated that at the peak of the first wave of the pandemic, up to 60% of the adult population of the UK were working from home; roughly 30 million people. For context, 2019 saw just 1.54 million people working from home in the UK as part of their main job .

2.1 IMPACTS ON DATA SECURITY, PRIVACY, & OTHER REMOTE WORKING ISSUES

The rapid switch for employees to relocate from in-office work, to remote working has raised an array of issues. One of the most concerning for both businesses and individuals revolves around protecting data and privacy. The almost instantaneous shift to remote working for such a large segment of the working population has resulted in several data protection and privacy issues. First and foremost, cyberattack levels have risen considerably since the start of the pandemic in March 2020. Many of these attacks have been themed around Covid-19, utilising fear and interest in the pandemic to find weakness in both business and individuals' cybersecurity.

According to Zscaler's recent research piece, "2020 State of Encrypted Attacks", Cyberattacks over encrypted channels increased by 260% in the first nine months of 2020. Based on insight sourced from over 6.6 billion encrypted threats across the Zscaler cloud, the company was able to show emerging threats from thieves who were utilising encrypted channels to bypass legacy security controls.

"The study found that following healthcare, the top industries under attack by SSL-based threats were finance and insurance (at 1.2 billion threats, or 18.3%), manufacturing (1.1 billion, 17.4%), government (952 million, 14.3%), and services (730 million 13.8%)."

In addition, a recent study by CrowdStrike, analysing threat activity on networks belonging to its customers, showed more intrusion attempts in the first six months of this year than in all of 2019. CrowdStrike blamed the pandemic-related shift to remote work, as well as the growing availability of ransomware-as-a-service for the uptick.

"Incidents of hands-on-keyboard intrusions in the first six months of 2020 — where a threat actor is actively engaged in malicious activity — was some 154% higher than the number of similar instances that CrowdStrike's researchers observed in 2019."

Interestingly, data from Microsoft's June 2020 blog, "Exploiting a crisis: How cybercriminals behaved during the outbreak" revealed that the surge in Covid-19-themed attacks was really a repurposing from known attackers using existing infrastructure and malware, but with new lures:

"These cybercriminals even targeted key industries and individuals working to address the outbreak. These shifts were typical of the global threat landscape, but what was peculiar in this case was how the global nature and universal impact of the crisis made the cybercriminals' work easier. They preyed on our concern, confusion, and desire for resolution."

Figure 2: Key statistics relating to cyberattacks in 2020



Source: Zscaler, CrowdStrike

02 Market Dynamics: Changing Attitudes & The Future of Work

Additionally, Microsoft found that cybercriminals were focussing on adapting their tactics to take advantage of local news and events that were more likely to lure victims to their schemes. In enterprise-focused phishing attacks this often looked like expected documents arriving which then required the user to take action.

The Association of Certified Fraud Examiners (ACFE) noted an increase in fraud cases reported by their contributors: "Seventy seven percent of our respondents said they've seen fraud go up since Covid-19 came on the scene, and they're expecting that to keep going. 92% expect they are going to see even more fraud over the next 12 months... We hear law enforcement, corporations, and individuals talk about how they're getting more and more attempted ransomware attacks or business compromise schemes."






Further, ACFE's research recognized identity theft and employee embezzlement as two of the five categories seeing the largest growth, in terms of increasing instances of fraud, compared with an earlier survey in May.

"With remote work, it's increasingly hard to ensure that the controls that were put in place are still operating appropriately or even still make sense. Thinking about protecting your intellectual property, customer lists and credit card information; when you are in an office, you have physical security measures, making it easier."

Understandably, the rise in remote work and the potential impacts this may have on data protection, has raised concern with regulatory bodies across the globe. In terms of official guidance, in the UK the ICO (Information Commissioners Office) has outlined 10 key recommendations as below:

Figure 3: ICO 10-point recommendations: "How do I work from home securely?"

-  1. Follow your organisation's policies, procedures and guidance
-  2. Only use approved technology for handling personal data
-  3. Consider confidentiality when holding conversations or using a screen
-  4. Take care with printouts
-  5. Don't mix your organisation's data with your own personal data

-  6. Lock it away where possible
-  7. Be extra vigilant about opening web links and attachments in emails or other messages
-  8. Use strong passwords
-  9. Communicate securely
-  10. Keep software up to date

Source: ICO

Further explanation from the ICO, as well as our assessment of the risks and subsequent impacts which have led to these recommendations being made, are as follows:

1. Follow your organisation's policies, procedures, and guidance.

"Your organisation will have adapted their approach to ensure that data is adequately protected. Avoid the temptation to do things in a way you think is more convenient, such as sending emails through your personal account or using the video conferencing app that you use with friends for work calls." - ICO

One of the major issues with the pandemic-driven switch to remote working, is that not only was it sudden, it was also widely believed to be temporary (many businesses planned for this to amount to a number of weeks, rather than many months). As a result, many institutions had not properly equipped staff or prepared their organisation. This involved inappropriate use of devices (reliance on employees' personal equipment), failure to address end-point security issues, and lack of staff training for cybersecurity issues.

Ultimately many business continuity plans have failed to address and prepare for a pandemic event such as Covid-19. This, coupled with the belief that the remote working switch would be temporary, has meant that business has lagged in addressing data security and privacy issues. In fact, survey data from B2B International, sourced in May 2020, showed there were exceptionally low levels of preparedness for a public health crisis: "Only 7% of firms stated they had plans that were designed for a pandemic specifically and which were fit for purpose. Indeed, almost a quarter of businesses reported not being prepared at all. A further 33% admitted they could have done much more to mitigate the effects of Covid. In total, almost 3 in 5 companies (57%) were on the side of being relatively unprepared."

2. ONLY USE APPROVED TECHNOLOGY FOR HANDLING PERSONAL DATA

As mentioned above, the sudden switch to remote working has meant that many organisations have relied upon their employees working from personal devices. A recent Trend Micro survey found that more employees have been fulfilling professional duties on personal devices, to the point at which almost 40% of workers across 27 countries are now relying on their own laptops, mobile phones and tablets for business needs.

"If your organisation has provided you with technology such as hardware or software you should use it. This will provide the best protection for personal data." - ICO

Ultimately, failure to supply and use company devices poses risk not only in terms of data protection, but also privacy, especially in instances where companies are using employee monitoring software (discussed further in segment 2.1 i b).

Some of the issues with so-called BYOD (Bring Your Own Device) are as follows:

- Out of date software (including the operating system) may be vulnerable to exploitation including loss or compromise of personal data.
- Devices are likely to be shared between family members. Other family members may see personal data that they should not have access to.
- Data is unlikely to be encrypted on the device and may be vulnerable in the event of loss or theft of the device.
- Inadequate access control, e.g. weak laptop passwords, may result in personal data being easy for unauthorised individuals to access.
- Data can easily be moved to other insecure storage (personally-owned USB sticks and external hard drives), increasing the potential for loss.
- Staff usage of insecure methods to communicate, such as personal email accounts, may result in compromise of personal data.

A potential solution is for employees to use their own devices, but to access company software:

- Consider using MFA (multi-factor authentication) for remote access.
- The device owner's data and the organisation's data should be separate. Staff should not be able to inadvertently or deliberately move the organisation's data onto their personal storage on the device or onto separate personally-owned devices.
- Organisations need to be aware that the device's security posture may be compromised, and make plans accordingly, e.g. out of date and unpatched operating system or security software.

3. CONSIDER CONFIDENTIALLY WHEN HOLDING CONVERSATIONS OR USING A SCREEN

As the ICO notes, there are many security risks around home working and confidentiality. For example, employees may be sharing their workspace with other family members or friends. This poses the risk that private or confidential business-related discussions may be overheard. Likewise, personal information or sensitive data may be easy to see on screen. So called 'Visual Hacking' is a significant concern and threat in today's remote working environment. The ICO recommends the following as basic guidance: "Try to hold conversations where they are less likely to overhear you and position your screen where it is less likely to be overseen." - ICO

Case Study: 3M privacy screens/filters

For many people, the ICO recommendation above is simply not possible, particularly where workspace is having to be shared during the period of national lockdown. In terms of on-screen security and confidentiality, this can be greatly enhanced with simple and easy-to-use privacy filters, such as those developed by 3M.

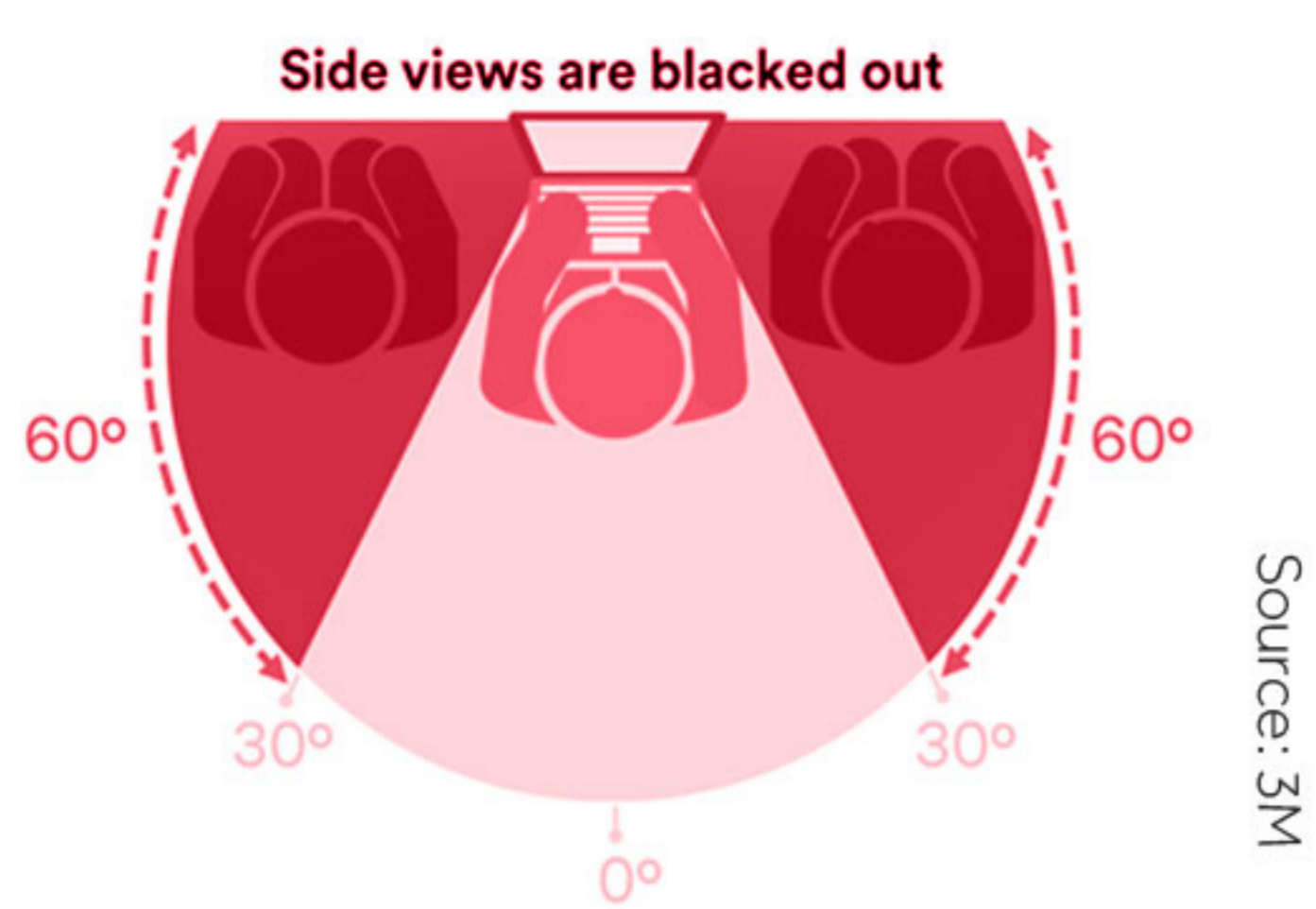
"3M™ Privacy Filters are removable display filters designed to shield sensitive data from prying eyes and are crucial to data security plans. Innovative microlouver technology from 3M prevents visual hackers' prying eyes from stealing your information and keeps data safe for intended users." - 3M

During this research, we reached out to 8 leading CISOs and executives who have previously spoken at PrivSec global events. These experts were given 3M™ Privacy Filters to trial on their work devices and were asked to feed back on their experiences; their opinion on the ease of use and overall performance of the technology. 3M™ Privacy Filters work by using microlouver technology to black out the screen from a 30-degree angle onwards, preventing viewing of the screen from sideways on. However, the filter still retains a crisp and clear view for the user sat directly in-front of the screen.



02 Market Dynamics: Changing Attitudes & The Future of Work

Figure 4 How 3M privacy filters work

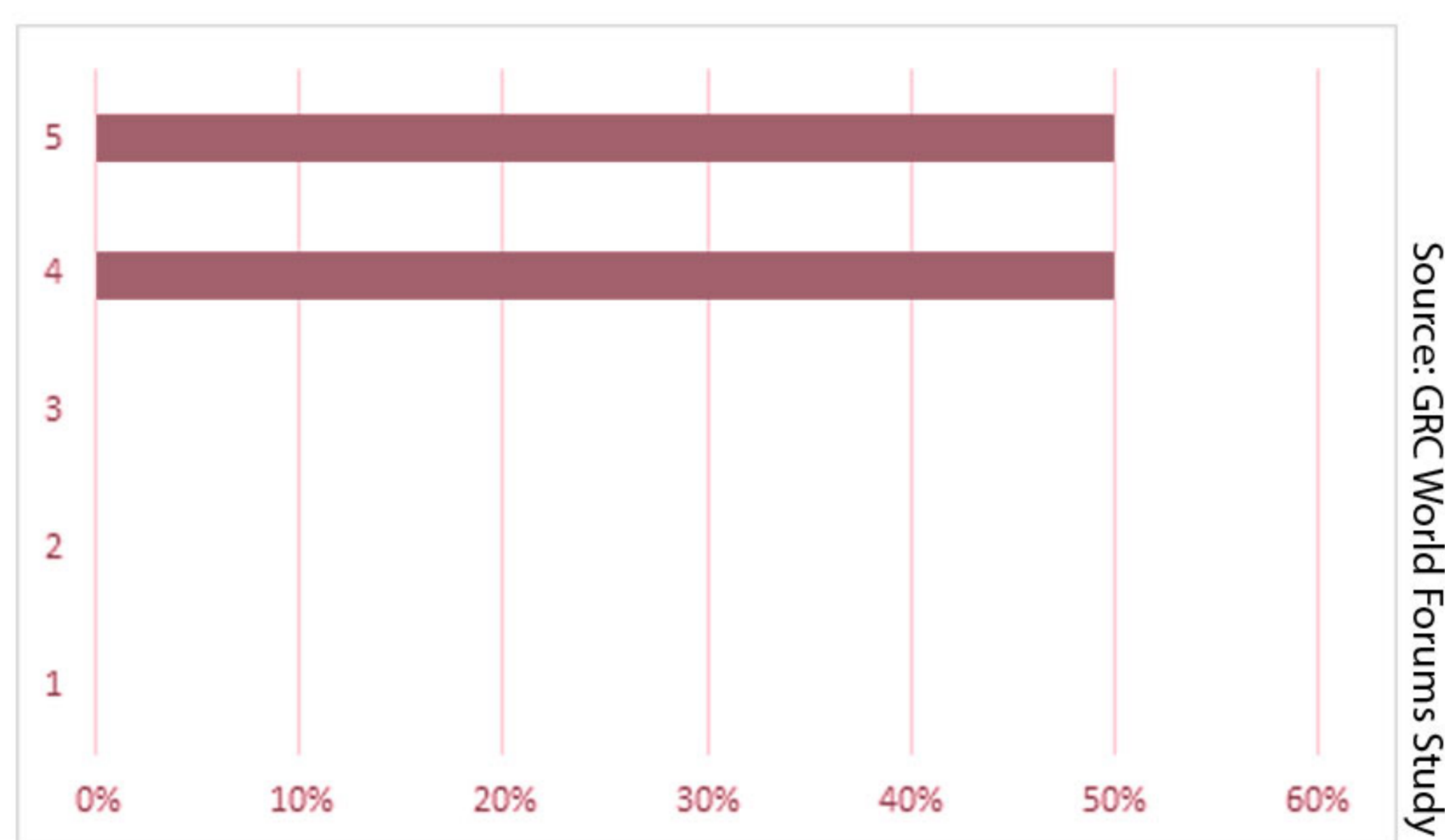


The consensus amongst our privacy experts, who we interviewed during the trial, was that the privacy screens were easy to install, with the majority scoring a 5 out of 5 for ease of installation.

"5 [out of 5] no issues at all." – Sawan Joshi, Head of Information Security, Firstport UK

"It was very easy to install without much to it." – Goher Mohammad, Head of Information Security, L&Q Group

Figure 5: Interviewee ratings of 3M privacy screens/filters in terms of the ease of installation (5 being very easy, 1 very difficult)



However, there was discussion on the initial positioning of the device, with Neil Sinclair, National Cyber Lead, Police Digital Security Centre telling us: *"No apparent issues, although adhesive strips give no leeway for error, 4 [out of 5]."*

Goher Mohammad made reference to the ability to reuse the screen:

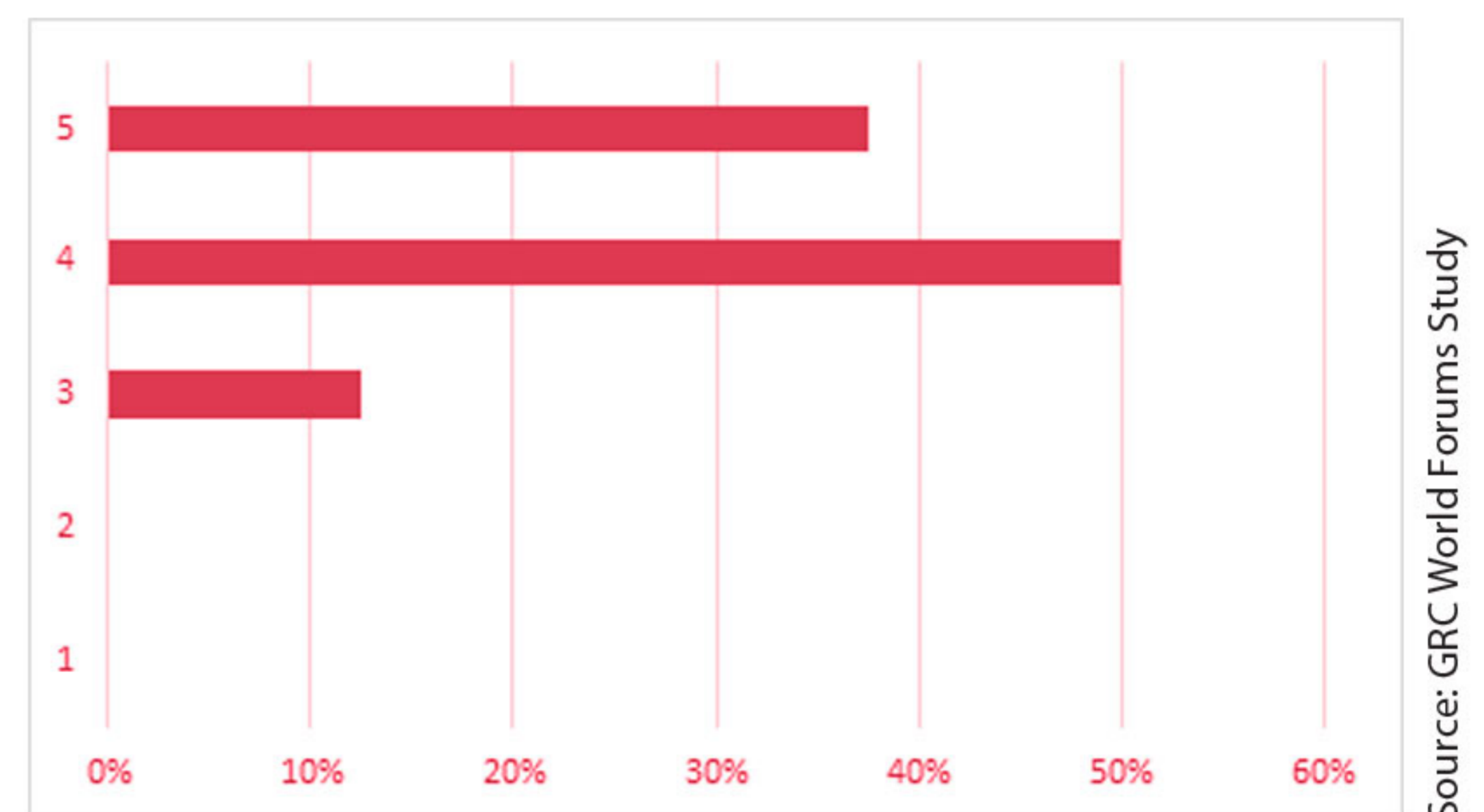
"The version I had was for the MS surface and it would be good to have the install which allows removal. The one I have feels like it must be permanently fixed to the screen"

We then asked our respondents whether they would recommend a 3M privacy screen device to a colleague, ranking this out of 5. Once again responses were very positive :

"5 – It is very lightweight, easy to install and does not affect the touchscreen." – Conan Chitham, Senior Privacy Counsel, MediaMath

"4 – It does add to a sense of privacy (I suspect this is greater on a laptop tablet – I am using mine on a big desktop)." – Neil Sinclair, National Cyber Lead, Police Digital Security Centre

"4 – An excellent relatively faff free way of ensuring some privacy whilst working in a public environment." – Glen Hymers, CISO, Save the Children



"I would recommend it for anyone who would like to work with more privacy in public. However, it still has limitations on its privacy. A special filter block filter with special glasses which allows viewing only to that of the person with glasses would give the most confidence." – Goher Mohammad, Head of Information Security, L&Q Group

There was, however, one slightly lower score of 3, as follows:

"3- I would recommend the screen while traveling, as for long-term working the screen fatigues your eyes." – Michael R. Büchler, Data Protection Officer – Nordics & Baltic, Manpower

Figure 7: Examples of a 3MTM Privacy Filters



The study then asked respondents whether they felt 3M's privacy screen removed the issue of visual hacking, as well as what they felt were the main benefits of the device, and whether there were certain tasks they would now feel more confident in completing remotely.

"Yes, [it does remove threat of visual hacking], substantially reduces the possibility of overlooking and means that I can manage client privacy more easily" – Conan Chitham, Senior Privacy Counsel, MediaMath

1. Q1 d) Did you have any issues whilst installing or using the screen? And, on a scale of 1 to 5 (1 being very difficult, and 5 being very easy), how would you rate the ease of installation of the screen?

2. On a scale of 1 to 5 (1 being very unlikely, and 5 being very likely), how likely would you be to recommend this device to a colleague? Why?

02 Market Dynamics: Changing Attitudes & The Future of Work

Richard Merrygold, Managing Consultant & Data Protection Officer, iSTORM®, agreed: *"Yes, the screen made it difficult for anyone sat beside me or approaching from the side to see what I was working on."*

Goher Mohammad stated: *"It would give me some confidence in a public environment, although I would still be mindful of those around me as there is still the ability to read from an angle."* He explained that the device helps with glare from the screen, and provides confidence when working in a public environment, adding: *"However, if I am working on a highly sensitive document, I would not be comfortable to rely solely on a privacy screen."*

Sawan Joshi told us: *"Definitely with this I can work more flexibly in public places; on a train; in a coffee shop and generally without concern. I do work on very classified cases due to the nature of my work and privacy is the main goal."*

Following assessment of the filters themselves, we asked our interviewees whether they had previously been taking steps to address so called 'visual hacking' prior to their use of the 3M screens. Many of our respondents spoke of limiting usage in areas where they felt privacy could be compromised.

Neil Sinclair, National Cyber Lead, Police Digital Security Centre, spoke of how he would position himself to avoid visual hacking:

"I always sat with my back to a wall, ensured passwords were automatically entered (if used at all), generally undertook no al/confidential/financial work in public."

Similarly, Goher Mohammad told us: *"I would reduce the usage of my laptop to where I felt confident I was not being overlooked or work on items which are not of a sensitive nature."*

This was also the case for Sandy Chan, APAC office, Rakuten: *"[I would be] working in a secure room, working with the wall to my back."*

This poses issues for business moving forwards, with a return to largely office-based work looking

Especially when we consider the potential for hybrid working, shared office space and hot-desking. As such, a solution like 3M's privacy screen can assist in protecting sensitive data and helping employees feel more confident working in 'the new normal, as well as providing reassurance for businesses owners and their customers alike'.

4. TAKE CARE WITH PRINTOUTS

The switch to remote working has meant that office policies have often been forgotten. Depending on the job role, workers may have access to sensitive data and personal information, such as that of customers or fellow employees. In an office environment, any printing of sensitive information would be covered by company policy and guidance in terms of both storage and disposal.

"At the office, it is likely you can use confidential waste bins. At home, you won't have that facility. Follow your organisation's guidance or safely store print outs until you can take them into the office and dispose of them securely." -ICO

A recent poll by records management firm Go Shred, of 1,000 UK adults working from home, revealed that 66% of respondents have printed confidential work documents on their personal printer. These included meeting agendas, commercial documents, payroll and CVs. The survey found that the average home worker prints five documents at home per week.

The study revealed that the top items being printed were:

- Meeting notes/agendas (42%)
- Internal documents including procedure manuals (32%)
- Contracts and commercial documents (30%)
- Receipts/expense forms (27%)
- Industry related copy (e.g. press release/brochure copy/articles/student work to proof) (24%)



"A fifth (20%) of home workers that have printed at home admit to printing confidential employee information including payroll, addresses, and medical information. 24% haven't disposed of printed documents yet as they plan to take them back to the office. 24% used a home shredding machine but then disposed of the documents in their own waste bin. 12% admit they have absolutely no knowledge GDPR regulations".

In the UK and the EU, GDPR covers personal data and requires businesses to have an effective, documented, auditable process in place for the collection, storage and destruction of personal information. Should any of these documents being printed at home ultimately be used to steal data, businesses could be found to have breached GDPR rules and face a significant fine.

As such, companies should make sure employees are aware and understand the implications of improper storage and disposal of sensitive documentation, as well as restrictions around what they may print. Company policies and guidance should be updated to reflect the switch to remote working, something which we believe is likely to prevail for several months yet.

5. DON'T MIX YOUR ORGANISATION DATA WITH YOUR OWN PERSONAL DATA

"If you have to work using your own device and software, keep your organisation's data separate to avoid accidentally keeping hold of data for longer than is necessary. Ideally, your organisation should have provided you with secure technology to work with."
-ICO

There is a risk that the use of personal devices could see sensitive data downloaded and stored, even when this is not necessary, thus ultimately posing a security risk. Additionally, such data could easily be forgotten meaning that it would breach GDPR restrictions around data retention. This highlights the need for businesses to inform and remind employees about their responsibility to safely manage data.

A potential solution here could be to use remote access for business software and documents, removing the need for employees to save data and files on their personal devices, thus effectively taking away the risk of redundant or sensitive data being left on a non-work device.

6. LOCK IT AWAY WHERE POSSIBLE

Being away from the office has also removed access to secure filing systems, as well as premises which are locked down at the end of the day: *"To avoid loss or theft of personal data, put print outs and devices away at the end of the working day if possible."* – ICO

This also links back to point 4, and the correct disposal of sensitive information. There is a very real and growing risk that personal data, both in print form and stored on devices is being forgotten and incorrectly stored across the workforce. Best practice and businesses rules around data protection have been lost or forgotten now that employees are not regularly in the office on a 9-5 basis.

7. BE EXTRA VIGILANT ABOUT OPENING WEB LINKS & ATTACHMENTS IN EMAILS OR OTHER MESSAGES

Don't click on unfamiliar web links or attachments claiming to give you important coronavirus updates. We're seeing a rise in scams so follow the National Cyber Security Centre's (NCSC) guidance on spotting suspicious emails. -ICO

As noted earlier in this research, the pandemic has seen a marked increase in cyberattacks. Worryingly, over 50% of security leaders in the UK and Ireland say their organisations experienced some form of cyberattack in 2020. This was according to a survey of security professionals conducted for Proofpoint by polling firm Censuswide. Further, more than 60% are concerned that they are at risk of attack in 2021, rising to almost 90% in the largest organisations. When looking at industry specific data, Financial Services firms were hit considerably by cyberattacks over the past year. 70% of these firms experienced a successful attack, with the majority blaming Covid-related conditions for the incident, according to Keeper Security. "Over half (57%) of respondents from Keeper Security's study argued that cyber-attacks are increasing in severity because of the move to work from home, and 41% argued that remote workers are putting the business at risk of a major data breach."

8. USE STRONG PASSWORDS

What may seem to be a basic part of cybersecurity, is often overlooked by both employees and employers alike. Weak and easy-to-guess passwords were responsible for 4 out of 5 data breaches in 2018, according to the 2018 Verizon Data Breach investigations Report.

"Whether using online storage, a laptop or some other technology, it's important to make your passwords hard to guess. The NCSC recommends using three random words together as a password (eg 'coffeetrainfish' or 'walltincake'). Make sure you use different passwords for different services too." -ICO

When we consider that a reported 80% of firms lack a password policy, this is a substantial area for concern, given how cyberattacks have increased in number over the past 12 months, and the workforce is scattered and disconnected more than ever before. Further, the use of personal devices by remote employees to complete work tasks, means they are even more likely to use the same personal password across numerous accounts, creating a much greater surface area for attack (arguably personal passwords are less likely to meet complexity required by business to prevent breaches).

9. COMMUNICATE SECURELY

Lack of in-office communication has led to employees relying more heavily on emails and video meeting software to address the removal of opportunity for face-to-face discussion and collaboration. Many workers were unfamiliar with the security issues using such tools, for example the risk of leaving Zoom meetings unprotected with a password, leading to so called Zoom Bombing (see section 2.2 c). Additionally, the increased use of email has led to staff sending unprotected documents and files between recipients. In many cases this is due to a lack of connectivity to business intranet, meaning that workers are saving files locally rather than on the companies drives. Lastly, password sharing is cause for concern. There are signs that users are actively sending passwords and account sharing to make things more efficient or access software they do not have installed on their own devices. Understandably this poses a significant risk to business security and operations.

"Use the communication facilities provided by your organisation where available. If you need to share data with others then choose a secure messaging app or online document sharing system. If you have to use email, which isn't always secure, consider password protecting documents and sharing the passwords via a different channel, like text." -ICO

10. KEEP SOFTWARE UP TO DATE

Given the significant increase in the surface area for cyberattacks, driven by the switch to remote working, (rise in the number of devices used by company employees for work), keeping software updated is paramount. Bad actors are rapidly changing and modifying their tools to launch cyberattacks, and software providers are ever releasing updates to combat any perceived weakness in their defences. Out of date software could make an individual significantly more at risk of cyberattack, and with employees using their own devices, companies have far less power to monitor the health of connected devices. Businesses should look at educating their employees in the importance of keeping their electronics updated, offer advice on protecting equipment, and where possible supply required technology, in order to mitigate risk.

"If you're using your own equipment, don't be an easy target for hackers. Keep your security software up to date to make it more difficult for them to get in. If your organisation has provided you with technology to work from home, this should be managed for you." -ICO

i. Further concerns with remote working

a) Working in public & using public Wi-Fi

There are several issues and security concerns relating to the use of public Wi-Fi, and whilst this has improved over the past couple of years, many company IT policies continue to state that work devices should not be connected to such networks. However, the pandemic has led to a convoluted situation, whereby some employees have found themselves reliant upon public access to the internet, often through their own personal device, but sometimes through work-provided electronics too. This situation has been born of necessity, as the pandemic and closure of offices has meant that some workers have sought to operate from locations such as coffee shops, to complete work.

02 Market Dynamics: Changing Attitudes & The Future of Work

There are many reasons for this: firstly, some employees suffer with the so-called 'digital divide' in terms of broadband connectivity, where certain rural areas are impacted by low internet speeds, rendering remote working solutions, such as video meeting software, at times unusable. In addition, the closure of offices has meant that couples and families are having to share internet connection, workspace, and devices. This has led to some workers getting out of the house to find somewhere else to work and be productive in environments that offer some of the social elements of the office space.

Even with improvement in the security of public Wi-Fi, cybersecurity professionals still recommend that public connections should be avoided during sensitive or business critical actions. There are a range of concerns relating to public Wi-Fi. For example, a malicious Wi-Fi hotspot could redirect a user to a malicious website. Connecting to a malicious Wi-Fi hotspot and then accessing something familiar, such as your bank's website, could lead to you being redirected to a phishing site impersonating your real bank. The hotspot could also execute what is known as a "man in the middle attack," loading the real bank website and presenting you a copy of it over HTTP. When you sign in, you would be sending your login details to the malicious hotspot, which could capture them.

It is recommended that for maximum protection (when public Wi-Fi use is unavoidable) a VPN (Virtual Private Network) should be used. In using a VPN, you connect to a single VPN server, with all of your system's traffic then being routed through an encrypted channel to the server. The public Wi-Fi network you are connecting to sees a single connection, your VPN connection and your online activity is hidden from all other parties.

Ideally organisations or businesses should make VPNs available to their employees, especially with the surge in remote working. However, consumers can choose to pay for a VPN service themselves to protect their internet use and their data.

There is also an alternative to public Wi-Fi. If you have a cellular data plan with wireless hotspot (tethering) capabilities and a solid cellular connection,

you could connect your laptop to your phone's hotspot in public and avoid the potential problems involved with the use of public Wi-Fi.

b) Flexibility, productivity & employee monitoring

The closure of many offices and the advice to work from home has led to a fundamental shift in how WFH is approached, both by business and individuals. Of course, the success and efficiency of working from home varies greatly between households, organisations and even industries. The pandemic has created additional problems, such as lack of childcare, the need to isolate for those in vulnerable groups, restrictions on daily life, etc. Therefore, it is not necessarily possible for all employees to work as efficiently as in the office, under current circumstances.

The reaction of businesses leadership to this crisis has been interesting and may well set out how the office of the future will be managed. There has been exploration of a range of solutions, including the direct monitoring of productivity. Other approaches have instead focussed on employee wellbeing, such as flexible start/finish times, additional breaks to enable employees to exercise, and changes to weekly hours to aid with home-schooling and childcare.

Data suggests that well before the Covid-19 outbreak, employees were keen to see the introduction and expansion of flexible work. FlexJobs' 2019 survey found that 30% of respondents left a job because it didn't offer flexible work, and further, 16% were looking for a job that offered flexible working

During the course of the pandemic, Nord VPN, a virtual private network service provider, has been tracking user behaviour, including when people log in to work. Their data suggests that U.S. workers are working three hours more per day than before the pandemic and subsequent lockdown. However, beyond an increase in hours, there are also signs that workers are taking the opportunity to work outside of office hours, potentially in an attempt to make up for unproductive periods throughout the day.

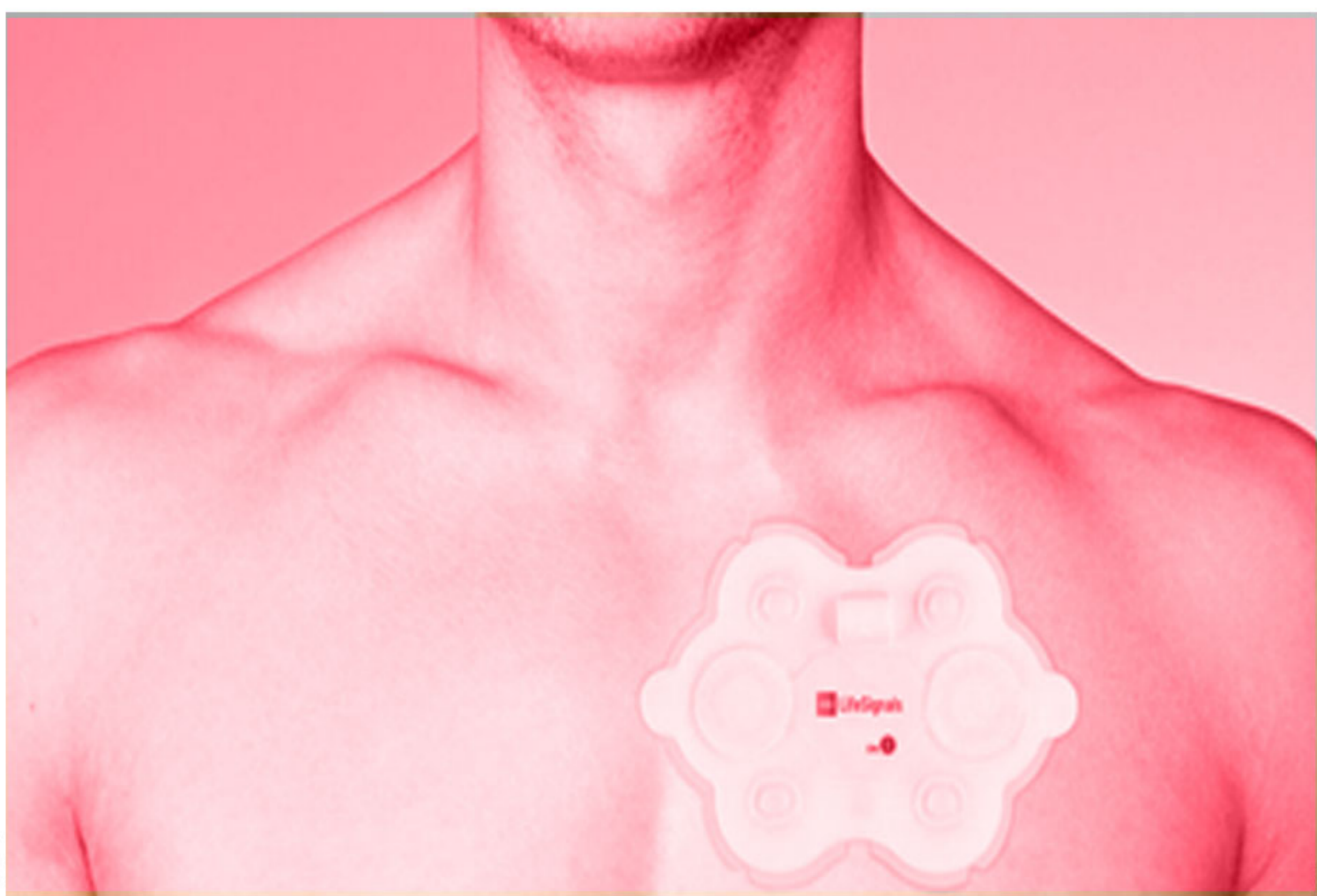


02 Market Dynamics: Changing Attitudes & The Future of Work

For example, Nord VPN's findings show that the peak time to send emails is now 9 am, compared to 10 am before the pandemic. In addition, the data also shows a spike in use between midnight and 3 am. Whilst Nord VPN cannot say precisely what users are doing during those hours, given that many people report they cannot work regular hours during the day due to family responsibilities, people may be utilising this time for work.

Worker health and wellbeing have also been under scrutiny, and while mental health is now becoming the focus of these concerns, at the start of the pandemic this was centred on making sure employees were not suffering from Covid-19. LifeSignals, a company that provides advanced multiple sensor interfaces for measuring a wide array of health-related data, initially created a monitoring patch to identify employees who may be suffering with Covid-19 symptoms. The device offers the potential for businesses to monitor the health of their employees, something which could be seen as overly invasive should it continue after the lockdown restrictions are eased and the pandemic's grip weakens.

[Figure 8: LifeSignals Health Monitoring Patch](#)



Advertising data raises concerns around privacy – questions around who has access to the information, and whether or not the data's use will be restricted to identifying the presence of coronavirus.

There is a risk that it could be used to judge employees who are suffering an as yet unidentified health issue, with employers discovering this before the individual themselves. Data may also be used to monitor productivity, prompting concerns that the data could be leveraged to initiate disciplinary procedures.

In other areas, companies have indeed focussed on driving productivity, but not from health monitoring tools; the pandemic has led to a surge in usage of so called 'time management software'. Products such as Time Doctor and Click Time allow employers to register productivity, either by recording which programmes are being used, or allowing manual input of project time by users. Some even go as far as to take intermittent screenshots of the employee's screen whilst they are working, or record keystrokes and clicks of the mouse.

There will be increasing concern that with WFH, work and personal life are blending into one, and previous boundaries between the two are being substantially eroded. With the introduction of productivity monitoring, businesses also risk accidentally recording the personal use of devices, for example during lunch breaks or after hours. This will be especially controversial in instances where employees are using their own PC or laptop but have been asked to install productivity monitoring software by their employer. Should sensitive information, or personal data be recorded (for example in screenshots taken), the organisation could face legal action.

Further to concerns with the work/life balance, software company, Atlassian, has been monitoring workforce behaviour. The firm found that more than half of respondents said it is now harder to maintain work-life boundaries, and 23% think about work after hours more than they used to.

These findings are supported by a recent study in Australia which surveyed 10,000 people working from home. The Australian Council of Trade Unions (ACTU) survey showed :

- 40% are working longer hours, many 5+ extra hours per week
- 90% not paid overtime or penalty rates
- Average \$530 (£291.92) per person additional expenses incurred
- 30.9% said they have an increased workload
- Almost half (49%) of those working from home have experienced some form of mental illness.

The study revealed that many home workers are working more hours, not getting paid for all hours worked, incurring significant work-related expenses, suffering mental health problems and have a worse work/life balance.

Atlassian suggest that companies will need to look at setting strict policies that guard against potential burnout. Such policies might include dedicated wellbeing check-ins, regular mandated breaks and a prohibition on after-hours communication. Likewise, the ACTU study recommends a charter for homeworking.

We asked our 3M study respondents how their working habits have changed during the pandemic. Worryingly, almost all of our respondents stated that their working hours had in fact increased, and some also noted a decline in the length and frequency of breaks taken:

"I have definitely been more productive but also started working longer hours. I am trying to get back to a better balance." – Goher Mohammad, Head of Information Security, L&Q Group

"The number of meetings has gone up, working hours have fluctuated – but generally gone up as well" – Sandy Chan, APAC office, Rakuten

"The whole team are working from home. Frequency of team meetings has increased from monthly or bi-monthly to weekly; work hours now generally include what was previously commute time [so longer]. [Also, I have] shorter and fewer breaks." – Neil Sinclair, National Cyber Lead, Police Digital Security Centre

However, there was positivity around the flexibility home working has offered:

"I am more flexible and feel happy to work proportionately every day, as it's all in my own control." – Sawan Joshi, Head of Information Security, Firstport UK.

"I am in a lot more meetings but enjoy having the flexibility and agility to work depending on the needs. It has allowed more time at home too with my family." – Goher Mohammad, Head of Information Security, L&Q Group.

"Days seem to start later due to saving [time from] office/business travel." – Michael R. Büchler, Data Protection Officer – Nordics & Baltic, Manpower

2.2 SECTOR SPECIFIC CONCERNS & EXAMPLES

In this segment, we have analysed some of the specific data protection and security issues faced, given the shift to remote working and learning processes during 2020. Whilst these are specific to certain sectors, there are lessons for the wider employment market and for businesses potentially facing a longer term move into remote working practices.

i. Education

Sadly, the rapid shift from in-person learning to virtual learning has exposed many flaws in privacy processes of not only Education Technology (EdTech) providers, but also the institutions which utilise them. Privacy advocates and education experts worry the increased reliance on EdTech tools has forced parents to choose between keeping their children's schooling on track and protecting their civil liberties.

What is EdTech?

"Educational Technology, or 'EdTech', is the use of modern technology to deliver education; applying digital technology to deliver a new form of learning architecture. EdTech itself is not a new concept, rather recent events, alongside technological advances, have helped to speed up adoption. EdTech has been presented as an important evolution in teaching since the turn of the millennium. It is also important to understand that EdTech is not purely a term for the technology involved, but also encompasses the learning techniques associated with this digital environment."

According to Check Point Software Technologies, the pivot by schools and universities to large-scale use of e-learning platforms has led to increased cyberattacks, "with the sector experiencing a 30% increase in weekly attacks during the month of August 2020." We believe that issues and the response by institutions could provide lessons for businesses in other industries. Whilst not a new occurrence, (the very nature of EdTech means it is, of course, as vulnerable to cyberattacks as any other internet-driven industry), the surge in EdTech adoption during the pandemic has led to a marked increase in such attacks.

Examples of some of the key cybersecurity threats are outlined below:

a) DoS (Denial of Service) attacks

As defined by CISA, DoS attacks "occur when legitimate users are unable to access information systems, devices, or other network resources due to the actions of a malicious cyber threat actor. Services affected may include email, websites, online accounts (e.g. banking), or other services that rely on the affected computer or network. A denial-of-service condition is accomplished by flooding the target host or network with traffic until the target cannot respond or simply crashes, preventing access for legitimate users." Separately, bad actors may use DDoS attacks (distributed denial-of-service) "where multiple machines are operating together to attack one target. DDoS attackers often leverage the use of a botnet—a group of hijacked internet-connected devices to carry out large scale attacks. Attackers take advantage of security vulnerabilities or device weaknesses to control numerous devices using command and control software. Once in control, an attacker can command their botnet to conduct DDoS on a target. In this case, the infected devices are also victims of the attack."

Recommendation: look at DDoS mitigation and recovery to help filter out such attacks, as well as how the business will respond, should services be brought down. Solutions may be cloud-based, or could be delivered on-premise via a filtering device placed in front of the network.

b) Ransomware

Ransomware is a form of 'malware' – malicious software. The software encrypts a victim's data until the attacker is paid a predetermined ransom, usually in cryptocurrency such as bitcoin. Only once the ransom is received will the attacker send a decryption key to release the victim's data. According to Cisco, "Ransomware is typically distributed through a few main avenues. These include email phishing, malvertising (malicious advertising), and exploit kits. After it is distributed, the ransomware encrypts selected files and notifies the victim of the required payment."

Recommendation: in the first instance there should be a recovery plan in place should a ransomware attack occur. IT staff should then follow these preparations to mitigate damage; this may include shutting down all systems to prevent propagation of the attack, enact disaster recovery (potentially through a 3rd party provider offering disaster recovery as a service), and find the source of the attack. Ultimately, end-user security is paramount in avoiding such attacks; the best way to prevent ransomware success is to train users and alert them to any new or emerging threats. Additionally, funding constraints and the scale of systems in place at schools often means that older devices are in use, thus creating environments that are more vulnerable to attack. It is paramount that IT departments patch and update devices as frequently as possible to ensure lapses in IT security are resolved. (Patching 3rd party software, which is commonly exploited, will prevent many attacks).

c) 'Zoom-bombing'

An expression which was unfamiliar until 2020, the term 'Zoom-bombing' has derived from attacks on the popular video conferencing provider, Zoom. The need for schools and businesses to move towards remote operations led to a surge in the uptake of Zoom and similar platforms in order to remain in touch with employees, deliver lessons, and to host meetings. Amid rapid adoption, security often became an afterthought – meetings were not always password protected, and attendees were not properly vetted. The result was attacks where bad actors, in the form of internet trolls, would join a meeting and interject profanities, pornography, sensitive information, or cause general disruption to scheduled meetings, leading to significant safeguarding issues for education providers. In some cases, targeted attacks on discussed on social platforms such as Reddit, have seen numerous users disrupting a single event. There are also concerns that Zoom-bombing is the latest technique being adopted in cyberbullying, making it even more difficult for schools to support bullied pupils.

Recommendation: The FBI made the following recommendations in March 2020, following a spate of disruptive and concerning Zoom-bombing attacks in schools:

- Do not make meetings or classrooms public. In Zoom, there are two options to make a meeting private: require a meeting password or use the waiting room feature and control the admittance of guests.
- Do not share a link to a teleconference or classroom on an unrestricted publicly available social media post. Provide the link directly to specific people.
- Manage screensharing options. In Zoom, change screensharing to "Host Only."
- Ensure users are using the updated version of remote access/meeting applications. In January 2020, Zoom updated their software. In their security update, the teleconference software provider added passwords by default for meetings and disabled the ability to randomly scan for meetings to join.
- Lastly, ensure that your organization's telework policy or guide addresses requirements for physical and information security.

d) Data theft

At the start of the pandemic, hackers were quick to hone in on the services that educational entities were turning to (such as Google Classroom). This made these distance learning services and any associated student data lucrative targets.

Hackers would seek to gain entry to school accounts on these platforms, often through phishing schemes.

Recommendation: When partnering with 3rd party vendors on EdTech, schools should consider the company's security policies, ensure that it has an incident response plan and consider the provider's policies on student data collection, retention and deletion, among other things. Additionally, staff and students should be made aware of best practices for IT security, for example creating stronger passwords, frequently changing passwords, and being aware of phishing emails.

ii. Healthcare

Case Study:

Cyberattacks on Educational Institutions

Ransomware: In the US, the FBI, CISA, and MS-ISAC have received numerous reports of ransomware attacks whereby malicious cyber actors target school computer systems, slowing access and, in some instances, render the systems inaccessible. Ransomware actors have also stolen, and threatened to leak, confidential student data to the public unless institutions pay a ransom. According to MS-ISAC data, the percentage of reported ransomware incidents against K-12 schools increased at the beginning of the 2020 school year. In August and September, 57% of ransomware incidents reported to the MS-ISAC involved K-12 schools, compared to 28% of all reported ransomware incidents from January through July. One example occurred in November 2020, where the Baltimore County Public Schools system was shut down by a ransomware attack that hit all of its network systems. The cyberattack brought classes to a halt for the 115,000 students attending classes entirely online due to the coronavirus pandemic.

Zoom-bombing: The FBI has received multiple reports of conferences being disrupted by pornographic and/or hate images and threatening language. The FBI Boston Division reported the following: in late March 2020, a Massachusetts-based high school reported that while a teacher was conducting an online class using the teleconferencing software Zoom, an unidentified individual(s) dialled into the classroom. This individual yelled a profanity and then shouted the teacher's home address in the middle of instruction. A second Massachusetts-based school reported a Zoom meeting being accessed by an unidentified individual. In this incident, the individual was visible on the video camera and displayed swastika tattoos.

Increased cyberattacks on UK Schools: According to analysis by Barracuda, 2019 saw almost as many cybersecurity incidents targeting schools as 2017 and 2018 combined. The research found that 83% of UK schools had experienced at least one cybersecurity incident in the past year. Data breaches were found to be the most common type of cybersecurity incident, accounting for 31% of total events, while malware came in second at 23%. However, it was also discovered that many UK data breaches in schools were not in fact carried out by malicious actors, rather they were accidental events.

02 Market Dynamics: Changing Attitudes & The Future of Work

As with schools, many healthcare infrastructures are reliant upon ageing IT and legacy systems, thus putting the data stored within their care at greater risk of attack. Combined with chronic underinvestment in cybersecurity, it makes for a digital environment which is both ill-suited for compliance with evolving legal frameworks, such as the EU's General Data Protection Regulation (GDPR), and under increased risk from increasingly intricate and sophisticated attacks by cybercriminals.

Digital transformation has added fuel to the fire, a point visible through a proliferation in medical gadgetry that is stretching cyber defences to breaking point. Analysis by Sensato finds that just 60% of medical devices are nearing their end of life with no further security updates available, while Forescout last year revealed that 71% of healthcare devices running on Windows were using outdated operating systems. Inadequate staff training and a lack of education about best practice in cybersecurity contribute to a working culture that is blind to the ever-present danger of data loss.

The coronavirus pandemic has brought the use of technology to the fore, as a tool to both aid in preventing the spread of infection as well as to help those suffering from the virus itself. Features such as contact-tracing and self-reporting apps have been widely used to identify, monitor and manage people who may have been exposed to the virus. As we enter a stage where businesses begin to reopen, especially with some return to physical office spaces, contact tracing, alert systems and potentially even vaccine passports, are set to become crucial tools in avoiding a return to restrictions.

Thus, it is likely that there will be a greater need to use personal data in order to monitor and assess the risk of an uptick in coronavirus cases as the economy unlocks. This will undoubtedly lead to a rise of targeted cyberattacks, as we have already seen over the past 12 months, though these may grow to centre on luring employees of companies, through spoof emails or ransomware, or even geotargeted attacks where a new variant or rise in cases may cause panic (and thus lower vigilance around suspicious emails or content).

By forcing an increase in the quantity of health data in circulation, the coronavirus has attracted the gaze of online criminals on the lookout for "evergreen" intelligence, as Frank Dickson, program vice president for security products at IDC stated:

"Healthcare data is...far more valuable than other kinds of data that can be accessed and exploited. When healthcare data is stolen, damage cannot be fully mitigated."

As he goes on to explain: *"A credit card can be cancelled or a bank account can be closed, but private patient data circulates endlessly which opens opportunities for various types of fraud to occur again and again from a single breach."*

Accordingly, cybercriminal activity has surged in the last nine months. Between January and April of 2020, private sector partners of INTERPOL detected 907,000 spam communications, 737 malware incidents and 48,000 malicious URLs, all of which were Covid-19 related. However, gaining employee consent to engage in tracking programmes or the sharing of health care data will be a challenge in itself: "Recent data suggests that even in the face of ongoing isolation and public-health threats, people still value their privacy, though they are split and understandably varying on whom they trust, with what information and for what specific purpose."

The Pew Research Center found in 2019 that nearly 80% of Americans said they were at least somewhat concerned about how companies were using their data. In another Pew study undertaken in April 2020, only 37% found it acceptable to track locations to enforce social distancing.





ROAD TO RECOVERY

03 Road to Recovery

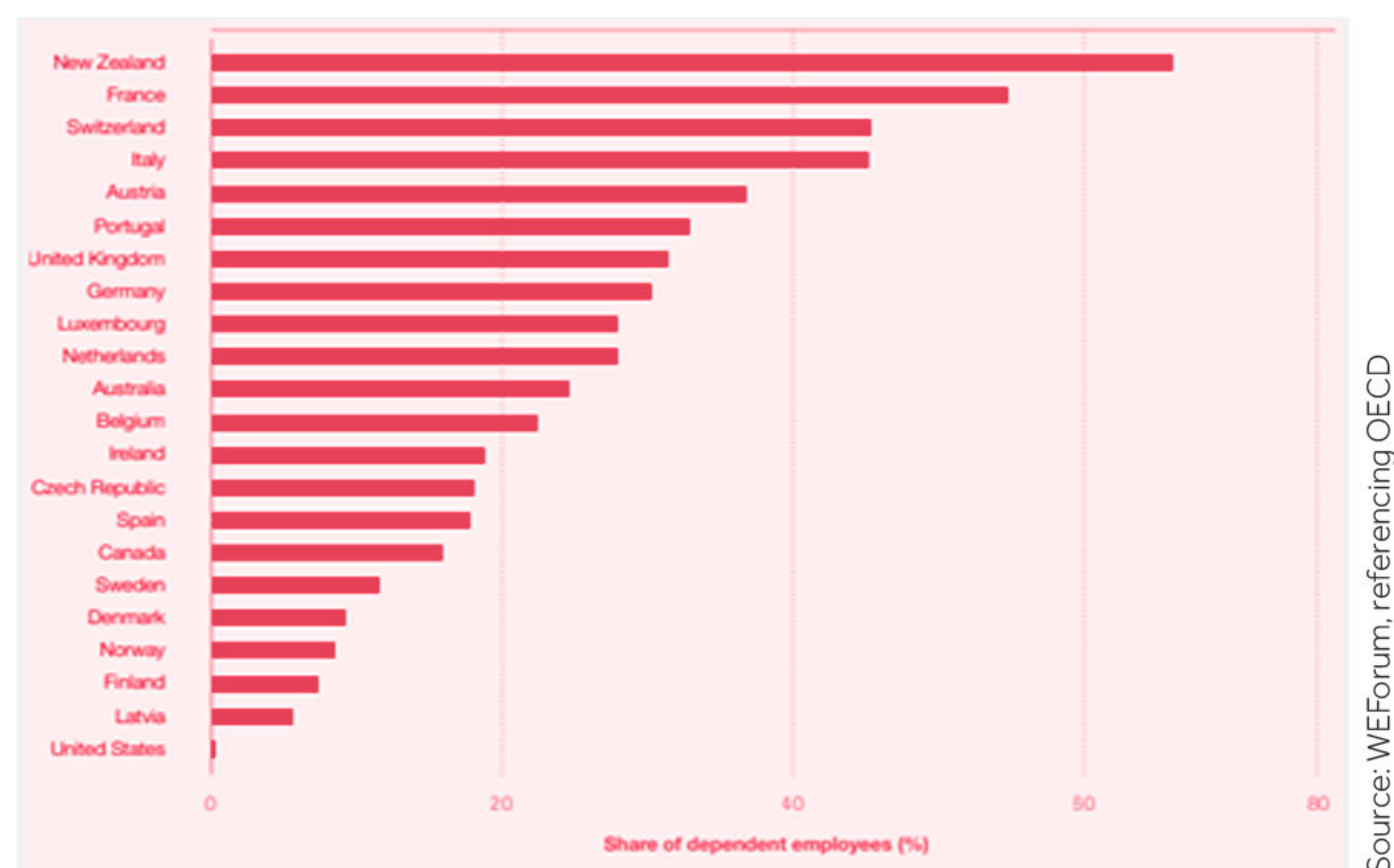
Over the coming months, it's likely we will see a gradual loosening of coronavirus restrictions, including those implemented on workplaces. The so-called road to recovery will bring focus onto productivity, establishing new work patterns, and returning to some form of 'normal'. This will centre around the ability for companies to operate increased in-person and face-to-face operations and allow employees the opportunity to come into offices or meet in other locations (potentially hot-desking facilities, hired meeting rooms, etc). This recovery, the impact on remote working, and what exactly the 'new normal' will look like, will be driven by the following factors:

a. The return of furloughed employees

Many nations have sought to support employment using furlough or wage subsidy schemes, helping businesses by paying a portion, or sometimes all of workers' pay whilst these employees are put on leave indefinitely. Examples include Germany's 'Kurzarbeit', France's 'Chomage Partial', and Ireland's 'Temporary Wage Subsidy Scheme'. These schemes aim to essentially freeze employment levels whilst the pandemic is at its peak.

After the first wave of the pandemic in spring 2020, many nations extended furlough schemes through to early autumn to protect workers from redundancy. In a positive sign for the UK scheme, the ONS (Office of National Statistics) reported that more than half of workers furloughed since May 2020, had returned to work by mid-August. "At the scheme's peak in May, 30% of the workforce across the UK was furloughed. The share of the workforce furloughed fell by more than half to 11% by mid-August." This will give hope for 2021, as we once again see restrictions lift, following the tightening of these through winter. The UK furlough scheme is set to end on September 30th 2021, the hope being that the vast majority of workers will be reintegrated into their current employment, thus giving a sign that the economy is opening up and productivity is accelerating.

Figure 9: Participation in job-retention schemes by country (proportion of dependent employees)



Source: WEFForum, referencing OECD

b. The return to the office

Following the first lockdown event, in the UK, there were signs in late summer that, as restrictions lifted, people began to return to the office. However official data from the week 24th August showed that trains entering the UK capital were carrying just "28% of their normal passenger loads, while the proportion stood at 45% for buses". Whilst recovery did begin in the UK, albeit slowly, the subsequent lockdown events of November 2020 and January 2021, have undoubtedly reversed this.

Other nations have been faced with a similar set-back. The emergence of more infectious and unknown strains of the virus, such as the Kent mutation, and the South African strain, have seen coronavirus cases soar across the globe since the Christmas period. Like the UK, many countries have been plunged once more into draconian lockdown measures, or have taken steps to reduce transmission, by directing people to work remotely.

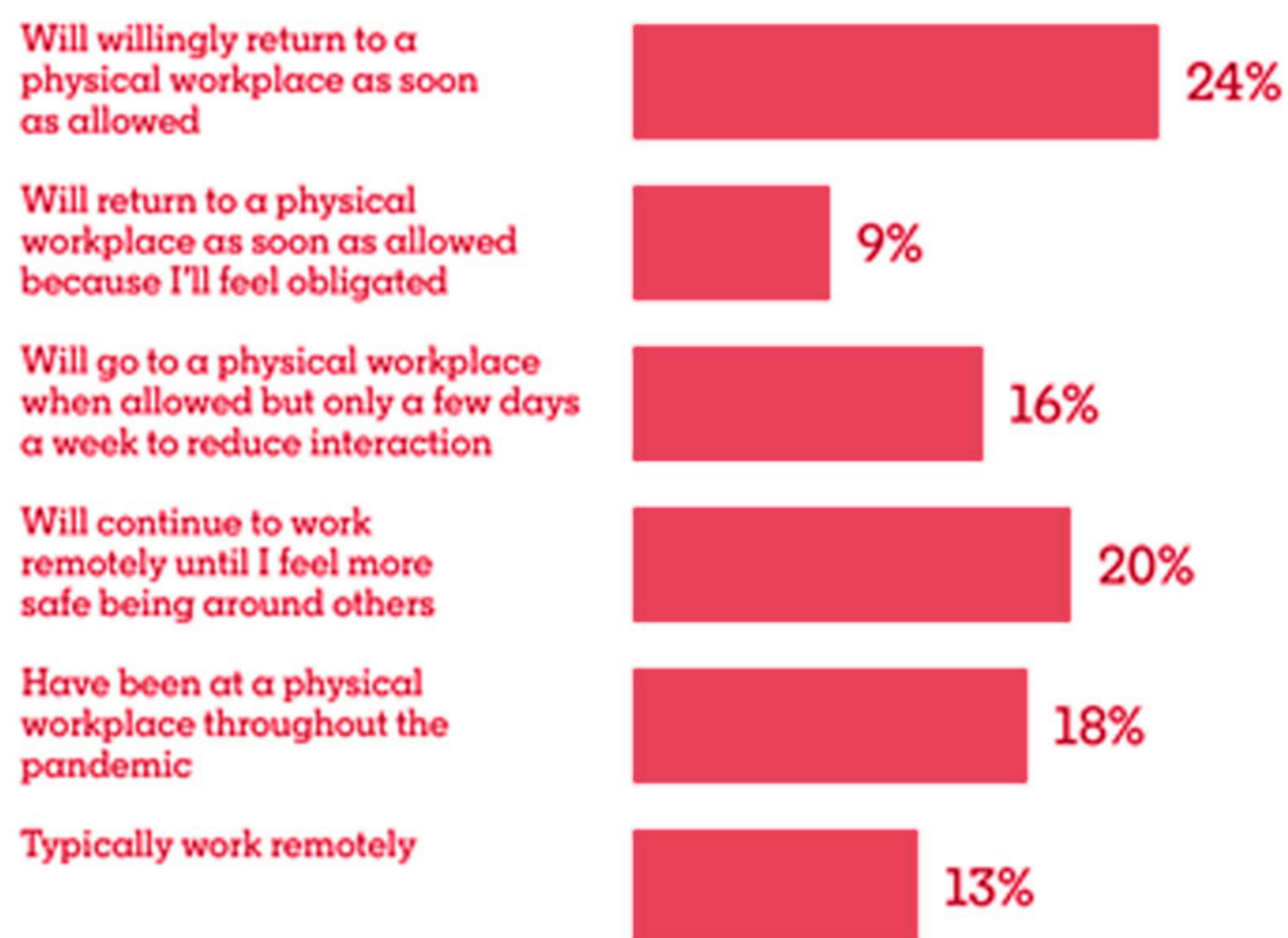
The result is that remote working will continue through much of 2021, with fears around safety and security in places of work heightened once more, given how transmissible these new strains appear to be. The longer remote working continues, the more complex we believe it will be for businesses to expect a full return to the older 9-5, office-based working environment.

Indeed, a recent global study of 2,500 workers by Wakefield Research for Honeywell found that 70% of respondents said they did not feel it was completely safe at their offices. Further, 24% threatened to look for a new job before returning to the office, if necessary safety measures were not implemented.

03 Road to Recovery

A study by LinkedIn in July 2020 (a period when life was beginning to return to normal as a result of reduced infection rates) saw just a quarter of respondent's state that they would willingly return to the office as soon as they were allowed.

Figure 10: LinkedIn study of UK attitudes towards returning to work



Source: LinkedIn Workforce Confidence Index research
Note: Percentages are calculated using a four-wave rolling average. 7,071 responses were collected between 1 June and 26 July.

LinkedIn News

Case Study: Planned return to offices by major US companies

The consensus among major US companies is for corporate employees to return in mid-summer 2021, once the vaccination programme has reached a broad segment of the population. Below we outline the recent indications from some of these employers, as to when, and how frequently their workers may return to the office. locations.

Apple



Apple CEO Tim Cook stated in December 2020 that it "seems likely" that the majority of teams won't be back in the office before June 2021. "There's no replacement for face-to-face collaboration, but we have also learned a great deal about how we can get our work done outside of the office without sacrificing productivity or results," he said, according to Bloomberg. "All of these learnings are important. When we're on the other side of this pandemic, we will preserve everything that is great about Apple while incorporating the best of our transformations this year."

Amazon



"We continue to prioritize the health of our employees and follow local government guidance," an Amazon spokesperson said in a statement to CNBC.

"Employees with work that can effectively be done from home can continue to do that work from home through June 30, 2021."

Microsoft



Fox Business reported that Microsoft was originally planning to return to offices in January 2021 but last October the company announced it was pushing its expected return date to July. In addition, Fox report that Microsoft announced plans to transition to a "flexible workplace" even after the pandemic is over. Kathleen Hogan, executive vice president and chief people officer at Microsoft recently stated in a Microsoft blog post: "For most roles, we view working from home part of the time (less than 50%) as now standard".

Facebook

FACEBOOK

"Regardless of when vaccines become available, we've given our employees the option to work remotely at least until July 2021. Our US offices remain closed and we don't expect them to open before the COVID-19 vaccines are widely available," Spokesperson for Facebook quoted in The Verge, 10th December 2020.

Another facet in support of a longer-term move to remote working is that many employees believe their productivity has increased since working remotely. A recent study by Nintex saw the U.S. company question 1,000 full-time employees at American businesses (with these varying in size between 501 to 50,000 employees). The study sought to identify whether workers are enjoying and embracing remote work. As Tech Republic reports, 70% of those surveyed by Nintex claimed that undergoing remote work amid the coronavirus threat was largely a positive experience.

"When asked to describe their better-than-expected experiences, respondents pointed to family time, no commute, fewer interruptions, and work-life balance."

03 Road to Recovery

Tech Republic noted that "67% of the employees from the survey reported they're getting their work done 'more efficiently since transitioning to full-time remote' but employees claimed they could benefit from 'additional flexibility, better tech equipment, and easy-to-use automation software.'" Further, "One respondent is quoted as saying 'compensation for Wi-Fi and more work materials that would have been provided in office' could be helpful, for instance, while others stated providing a more 'flexible work hour routine' or 'do not disturb time blocks' would make remote work run more smoothly."

The Nintex survey is not alone in identifying a perceived uptick in productivity. A 2021 survey of 200 businesses in Ireland, by technology company Expleo, found that: "89% of Irish business and IT leaders in Ireland said productivity had improved or stayed the same while working remotely during the Covid-19 pandemic. Additionally, 52% noted an improvement in productivity, while 37% reported a maintenance of productivity levels. Only 11% of respondents said productivity had declined due to remote working".

However, it is not all positive. The Expleo survey revealed "that 53% of respondents expressed concern that long-term remote working has impacted or will negatively impact their team or organisation's camaraderie". Hybrid models could help alleviate this situation by providing time for team building, and face-to-face socialising amongst co-workers in order to develop and maintain a sense of belonging and camaraderie. It will also likely support employees' wellbeing, enabling staff to engage socially, build broader support networks, and feel part of something bigger.

c. Office behaviour (potential switch to hot-desking, flexible hours)

As suggested by firms such as Apple and Microsoft, the return to the office is not likely to be clear cut. Rather than individuals coming back into the company workspace for the full Monday-to-Friday 9-5, a mixed approach is more plausible.

It has been suggested that not only will employees spend more time working remotely, but we will also see a change in how office work is conducted.

Having seen months of remote work, many businesses are reassessing the costs of office space, leading to reduced rates of leasing and ultimately a surplus of property.

In November 2020, the Financial Times wrote about how US technology firms in the Bay area of San Francisco, had seen a substantial increase in sublease space, driven by the switch to remote work. This increased by 148% through September 2020, according to Savills. Highlighting some of the notable contributors to this, the article stated: "In late August, Pinterest cancelled a 490,000 square-foot lease at a building it was developing in the city, incurring a charge of \$89.5m to do so. A month later Twitter put 105,000 square-feet of space up for lease. Earlier this year Twitter told employees they could work from home indefinitely if they desired."

We have seen similar signs from businesses in the UK, with multinational insurance provider Aviva, which employs 16,000 people in the UK (37,000 globally), revealing plans to close offices and focus operations in city centres. The company has said that the plans would not lead to job cuts and offices would still be available for staff on a rotation basis. It said it expected most staff to spend one day a week in an office on average. "The way we use our office space is changing significantly. We are combining office space in some locations and reducing the space in others. Our intention is to invest in our sites to provide a more vibrant, inspiring and flexible workspace for our people."

Employees coming into the office for just two or three days a week is one of the proposals Google and parent company Alphabet are considering. In a recent online event hosted by Reuters, Alphabet CEO Sundar Pichai told viewers: "It's one of the things I'm very excited by because I think it's going to drive a tremendous improvement in productivity over time globally, will also pull more people into the workforce who aren't able to be part of it today."

Thus, it is likely that hybrid models will prove popular with employers, at least in the initial drive to return to the office. Such formats (the mixture of a few days' remote work plus a few days in the office per week, coupled with more flexible hours) will help in encouraging employees back to office-based work. Many employees will remain cautious about the threat of coronavirus, even as the vaccine rollout accelerates.

03 Road to Recovery

Another potential positive is that such models will see a greater decentralisation of the workforce, meaning some industries will see job creation extended geographically outside more traditional locations, such as city hubs, thus spreading wealth and productivity further.

"With a more flexible future likely, the biggest challenge companies will have beyond safety concerns is how they can create inclusive workplaces and cultures that work for remote workers, hybrid workers, and office-only workers," Wired quoted Janine Chamberlin, senior director at LinkedIn, as saying .

d. Job creation, interviewing, and onboarding of new employees

A further area which has, and will continue to see disruption, is in the interview and onboarding process for new employees. During the pandemic, there has been great restriction placed on face-to-face interviewing, with much of this having been done remotely as a result. There will be concern that some jobseekers lacking digital access, or suffering from issues such as slow internet connection, may miss out on job opportunities. If business decides to continue remote practices, then we could see a digital divide form in employment.

Additionally, there are privacy concerns around the use of video conferencing software to interview. Many interview candidates will, or have been forced to interview from home. As a result, unfair judgements may be made about a candidate's suitability simply from what the interviewer has seen shown in the background of their call, or even from noise and disruptions such as a busy family life, especially where companies may be planning long-term remote working policies.

It is likely that the digital switch discussed above will extend into the onboarding and training of new workers, where much of this is likely to remain online for many more months. Employers will certainly seek to minimise unnecessary face-to-face contact that could put workers at risk of catching coronavirus, given an outbreak could be severely damaging to both productivity and to reputation. As a result, it's crucial that all business provides opportunities for those lacking in their digital set-up, as well as providing the necessary resources for new employees.

e. Opportunity for upskilling

There is a fantastic opportunity related to the above. However, with the switch to digital and remote working, business should aim to provide employees with new digital skills. Many older employees, or those in less digital-focussed roles, are at threat from a skills divide. Business can use remote working, and the likely switch to a hybrid model to address areas where there is a skills shortage; the training of current employees will create a more efficient and future-minded workforce. It can also be used to create new job roles and help workers to move up the ladder, particularly significant given the challenges we all face recovering from this global coronavirus pandemic.

THE OFFICE OF THE FUTURE: WAYS IN WHICH WORK MAY CHANGE

In this segment, we set out how the office of the future may look over the next few years, as we begin to exit the pandemic. We also identify areas where privacy will be of concern, and offer thoughts on how this may be addressed.

1) Hybrid office model and work life reimagined

As we discussed in the previous segment, the hybrid model is likely to emerge as a preferred way of working with employees and employers alike, especially as businesses try to get workers back into the office. This flexibility will help to satisfy the argument that many have found they are more productive working remotely but miss the social contact of being in the office. A balance will therefore be struck between several days at home to allow for focussed work on projects, with employees then in the office for a couple of days per week to attend meetings etc. We asked our interviewees about what they felt the longer-term impacts of the coronavirus pandemic would be on ways of working:

I think remote working will be more widely accepted. I also think offices still have a place but choice and freedom to be flexible will be the future for many businesses. – Richard Merrygold, Managing Consultant & Data Protection Officer, iSTORM®

03 Road to Recovery

Neil Sinclair believed there would be less use of office space and less social interaction (particularly within his team). Similarly, Sawan Joshi thought there would be less physical interaction which would impact upon social aspects within corporations, as well as there being a knock-on impact which would create an output-driven work environment in which delivery is much more visible.

"We will be working in an agile way where businesses will need to cater for flexible working. If businesses cannot provide this, they will struggle to recruit, whereas those offering flexibility will benefit from those seeking it. The pandemic has allowed workers to be at their home as well as work, and has enabled a balance which may not have been offered before. This way of working is here to stay." – Goher Mohammad, Head of Information Security, L&Q Group

It will be hard for employers to expect an immediate return to office life, if ever. According to polling from Gartner, 48% of employees expect to work from home post-pandemic, up from 30% pre-pandemic .

"Remote working is likely to be a permanent feature even if it is not full time." – Conan Chitham, Senior Privacy Counsel, MediaMath

In fact, many think that post-pandemic working life may be less about where employees work and more about a cultural change that sees companies offering their workers greater autonomy.

"Those that traditionally didn't think they could work from home will now continue to do so." – Glen Hymers, CISO, Save the Children

The benefits would be seen in the flexibility this offers to employees, as Wired recently explained: "Working parents may no longer have to seek permission before taking a morning off to attend to childcare needs, and junior employees may be able to work from home without worrying about the optics."

We believe that it is most likely that hours in physical office locations will be cut, leading to businesses seeking more shared-office space facilities in order to reduce rental costs. There are significant risks here relating to privacy.

For example, shared office space could lead to instances of corporate espionage, should businesses in similar industries work in the same environment. Access to such buildings will need to be secure and monitored. This draws upon our earlier discussion around tools to protect confidential information, such as the use of secondary devices such as 3M privacy screens, enhanced password protection of user accounts and data, and the need for training for all employees. The transition to a hybrid environment will not be without challenges, and it is paramount that companies make preparations as soon as possible.

2) An information technology revolution

The above switch to hybrid will likely require an IT revolution – an increase in recruitment of sector roles, as well as the updating of policies and practices. We believe the following will be seen:

a) IT skills drive

To address privacy concerns, as well as facilitate remote and decentralised business operations, there will need to be an IT skills drive. A recent survey of Irish business leaders, conducted by technology company Expleo, found that "12% of companies have increased headcount during the pandemic, while 35% of companies plan to hire more people to address their IT skills shortage over the next 12 months. Additionally, 30% plan to outsource more IT functions and 43% plan to automate more processes to deal with their IT skills shortages."

This will enable business to not only continue with aspects of remote working, but to update and maintain systems in this world of working, as well as aid with security in shared office environments, or circumstances where employees are working in public locations.

b) Enhanced IT policies to address changing work environments

Business must recognise that the pandemic and sudden switch to remote working was not a flash in the pan. Early on in the pandemic, many companies believed the switch to working from home would only prevail for a couple of months, rather than over a year.

03 Road to Recovery

This has resulted in many companies having to play catch-up, or working in less than ideal circumstances, apparent through IT policies that don't necessarily have the depth to cover such a set-up, or through employee training not being up to specifications in terms of what is required with a switch to out of office working (e.g. storage of data, adequate password protection, sharing of logins, and the correct disposal of print-outs and sensitive information).

We asked our interviewees about what their companies had been doing to enhance security whilst conducting remote work, a question that has yielded ideas that should prove interesting to other businesses.

"All workers have been issued with corporate laptops/PCs; all access to corporate property via virtual desktop with full perimeter security; full training provided on 'strengthening' home router security; employees advised to set-up 'work-only' Wi-Fi address on home router; employees advised to create 'Admin only' accounts on home PC to protect home network; re-written policy for public Wi-Fi use (basically limited to specific roles)." – Neil Sinclair, National Cyber Lead, Police Digital Security Centre

c) Return to company property rather than personal equipment

As Neil Sinclair referenced above, businesses should be providing workers with corporate devices for work use. The rush to switch to remote working saw many companies allow, or rely on, employees using their own personal devices. As we have discussed in the research, this raises a number of security issues, including a lack of secure passwords; a risk that company and personal data will be mixed and improperly stored; the use of personal email accounts for work, as well as concern that software and system updates are not current, potentially opening devices up to the threat of being compromised.

d) Agility of companies to facilitate home working

Should further outbreaks occur, or another pandemic event hit, businesses will now be far more flexible and reactive to such threats, in terms of their ability to work in a decentralized manner.

The processes to enact such a switch, which would have taken many years, have been achieved (albeit rapidly) over a matter of weeks and months. Whilst this has not always been perfect, companies have seen that remote work can be done successfully. Focus must now fall on enhancing efficiency and creating successful working environments for employees.

3) Surveillance & employee monitoring

As we exit the pandemic and some employees begin to return to the office, businesses will be closely monitoring employee health, eager to avoid an outbreak of coronavirus in their workforce. Several technological solutions are being looked at to help with this: "Temperature checks, distance monitors, digital "passports," wellness surveys and robotic cleaning and disinfection systems are being deployed in many workplaces seeking to reopen."

Examples according to This Is Money include :

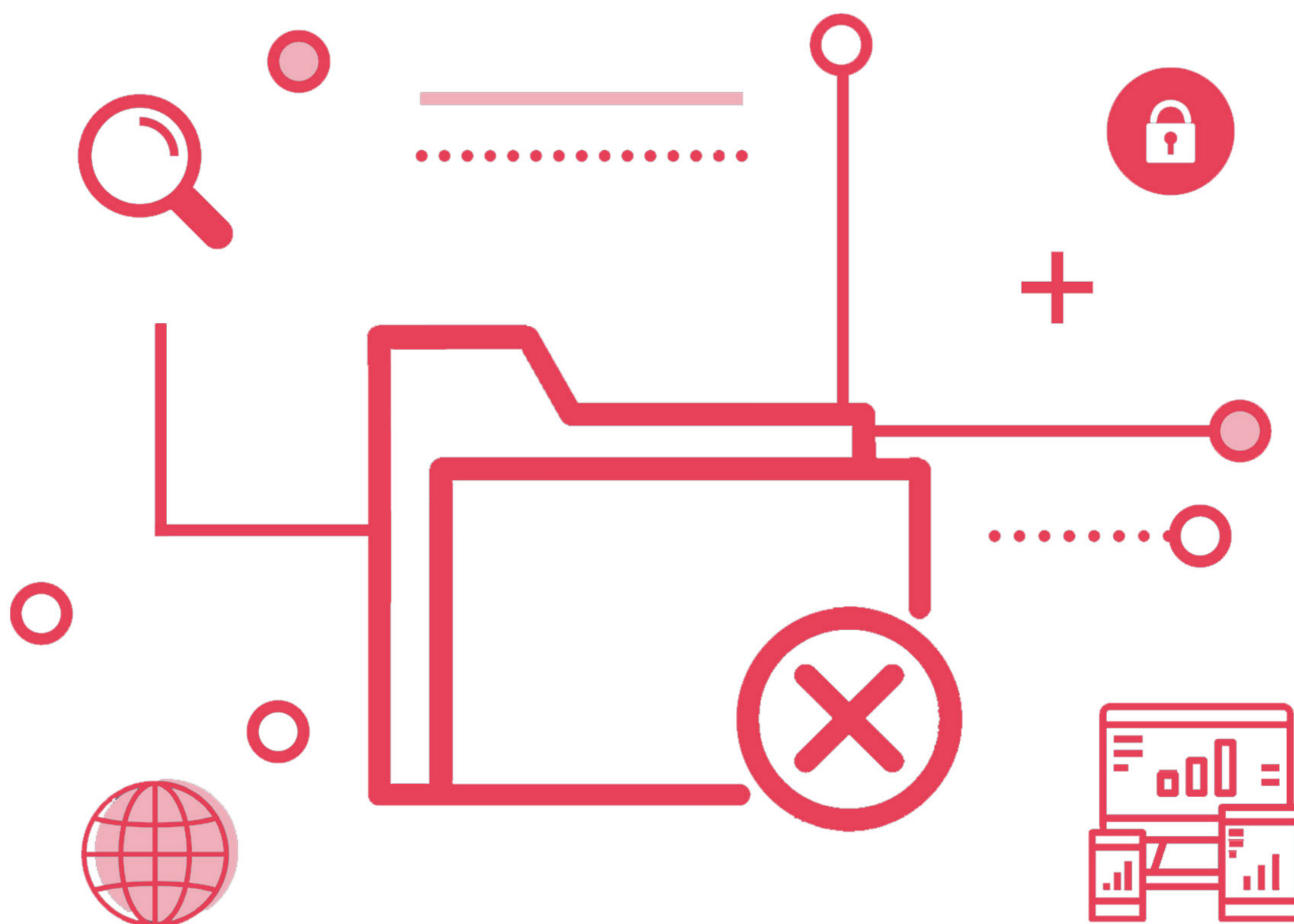
- Fitbit are equipping some 1,000 NASA employees with wearables as part of a pilot program which requires a daily log-in using various health metrics which will be tracked by the space agency.
- Microsoft and insurance giant United HealthCare have deployed a ProtectWell app which includes a daily symptom screener.
- Amazon has deployed a "distance assistant" in its warehouses to help employees maintain safe distances.

However, many of these solutions could be viewed as an invasion of privacy, and there will be concerns around the information they are collecting, especially where data on an individual's health is being recorded. Some solutions look to screen employees as they enter a building lobby, as well as monitor in elevators, hallways and throughout the workplace. This monitoring "blurs the line between people's workplace and personal lives." Darrell West, a Brookings Institution vice president with the think tank's Center for Technology Innovation, recently told This Is Money: "It erodes longstanding medical privacy protections for many different workers."

03 Road to Recovery

For those working remotely, there are increased concerns around employees overworking and working outside of office hours, where work boundaries are increasingly being blurred. As such there needs to be greater awareness and understanding of employee health, as well as clear boundaries created to reinstate the work/life balance.

It is likely, therefore, that we will see companies address this with new policies to reduce over-working and communication out of hours, unless employees have explicitly declared they are happy with this. It could even be that new legislation is required from government to protect workers. Further, it is likely that employee monitoring tools or virtual 'clocking-in' systems will see greater uptake, as employers seek to keep greater tabs on where and when employees are completing tasks.



References

Working from home (WFH) statistics 2020 | Finder UK

Ibid

Ransomware attacks over SSL increase by 500%, Zscaler report shows (securitybrief.eu)

<https://www.darkreading.com/attacks-breaches/more-cyberattacks-in-the-first-half-of-2020-than-in-all-of-2019/d/d-id/1338926>

Exploiting a crisis: How cybercriminals behaved during the outbreak - Microsoft Security

How do I work from home securely? | ICO

COVID-19: Almost 3 in 5 Businesses Admit They Could Have Done "Much More" To Prepare (b2binternational.com)

Study finds 39% of employees access corporate data on personal devices | 2020-09-14 | Security Magazine

Privacy & Screen Protectors - Privacy & Protection | 3M US

Printing work documents at home could land you with a GDPR fine | TechRadar

Homeworkers face fines for printing out documents, under GDPR | theHRD (thehrdirector.com)

Most Financial Services Have Suffered COVID-Linked Cyber-Attacks - Infosecurity Magazine (infosecurity-magazine.com)

Forget Data Privacy; 80% Of Firms Don't Even Have A Password Policy (cxotoday.com)

Is the Pandemic a Tipping Point for Flexible Work? | FlexJobs

<https://www.bbc.com/worklife/article/20201110-the-rise-of-employee-health-tracking>

<https://www.atlassian.com/blog/teamwork/data-analysis-length-of-workday-covid>

<https://www.examiner.com.au/story/7002435/working-from-home-actu-survey-looks-at-the-issue/>

A 'New Normal'? – Digital Privacy News

Official figures show that the furlough scheme has worked: saving jobs and helping more than half of employees back to work already - GOV.UK (www.gov.uk)

WEF_Future_of_Jobs_2020.pdf (weforum.org)

Government backing away from calls for mass return to office for UK workers | The Independent | The Independent

Company leaders prepare their return-to-office coronavirus vaccine policies (digiday.com)

References

Study: Workers say they are more effective working from home - TechRepublic

Productivity improved with remote working - survey (rte.ie)

Companies dump US office space at rapid rate | Financial Times (ft.com)

Aviva to close offices in hybrid working plan - Personnel Today

The Covid-19 vaccines will usher the dawn of the true hybrid office | WIRED UK

Build the Workforce You Need Post-COVID-19 (gartner.com)

The pandemic is giving people what they want: flexible working | WIRED UK

<https://www.rte.ie/news/business/2021/0122/1191366-expleo-survey-on-remote-working/>

Privacy faces risks in tech-infused post-Covid workplace | This is Money