Secure your customer experience staff working from home.

verizon

Customer experience: The new frontline in cybersecurity?

Just a short while back in 2018, it was suggested that the growth of homeworking had stalled with only 6% of the UK's workforce working from home.[1] It's not hard to see why: working from home has typically been limited to a select few – those working in the technology sector, those required to travel extensively – people that could essentially work remotely from anywhere. It wasn't something a typical contact centre employee could do. But it was something employees were interested in, and something that businesses have been contemplating for years.

The COVID-19 pandemic caused a lot of businesses to rethink how they worked, and in a very short amount of time. Where they may have been reluctant to allow working from home in the past, they had little or no choice during the national lockdowns. It was the only way to maintain customer experiences. Sales and support staff were suddenly able to work from almost anywhere, with voice, video and host systems integrated. And what's more – it worked.

Looking ahead, employers expect that once the crisis is over the proportion of people working from home on a regular basis will double.[2] With the workforce now quite literally mobile, businesses can't be complacent about remote worker security. In the past, many businesses had failed to take it seriously and regularly cut corners, making them one and a half times as likely to suffer a mobile related compromise.[3]

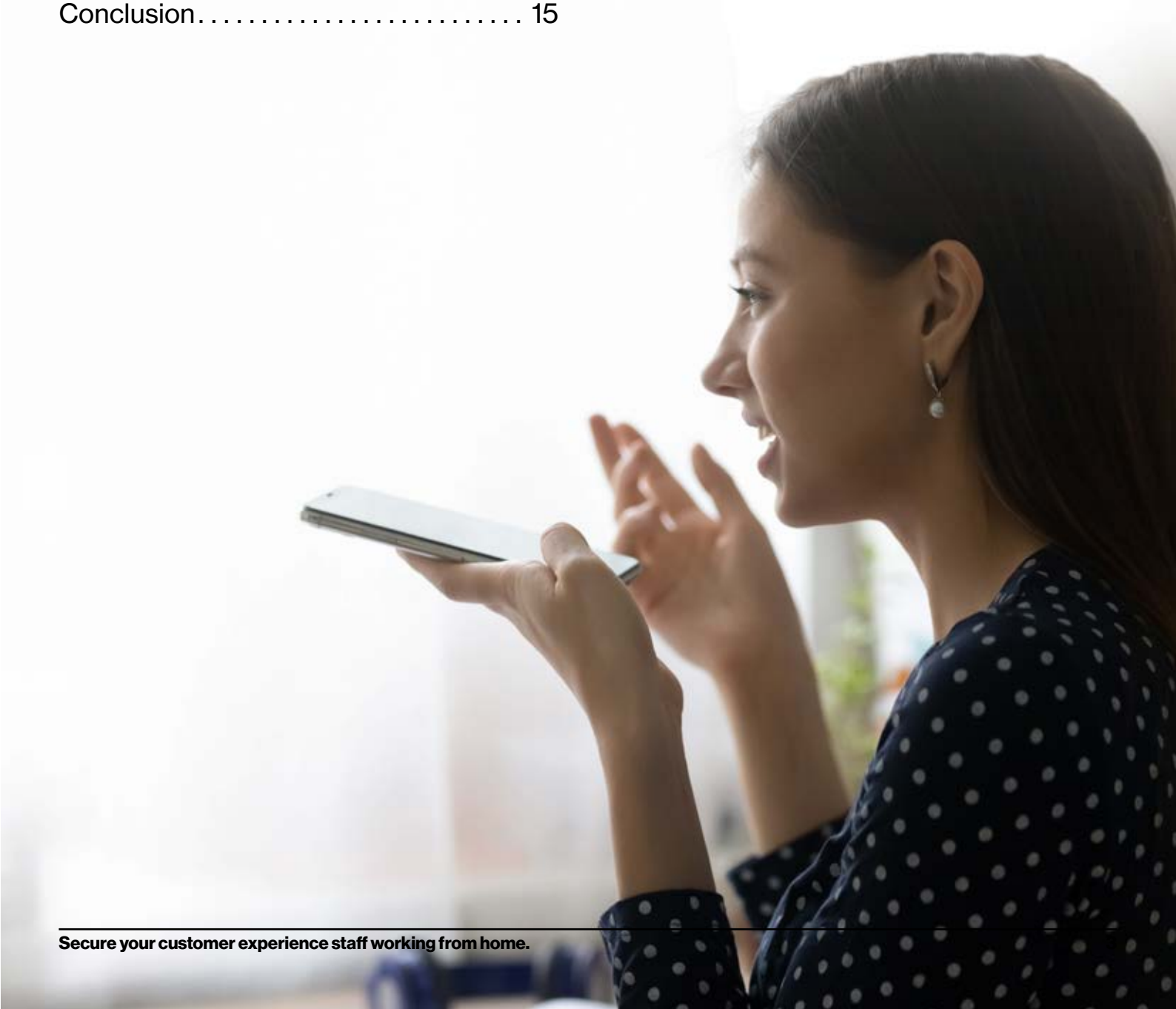
A security compromise can be a costly business – remember fines for a data breach under the EU's General Data Protection Regulation (GDPR) can be up to 4% of an organisation's global turnover. And the EU isn't alone in introducing comprehensive privacy legislation, several US states including California, Nevada and Maine have followed suit. But it isn't just fines; a data breach can have an adverse effect on a businesses' reputation which can lead to a further loss of revenue down the line. That's on top of the cost of any time lost remediating a breach.

Working from home is appealing for many because of the flexibility it offers. Unfortunately, that mentality sometimes spills over and leads to behaviours that impact security. Employees can unknowingly put their employer and its customers at risk.

The workforce looks set to be at home for years to come, it's time to give them the tools to do it safely. In this report we'll discuss the biggest security challenges facing home workers.

The recommendations in this report could help you to mitigate the risk. This will help you to continue to provide excellent customer service, without jeopardising your company's reputation or financial security.

Contents



Barriers to adoption?

Companies that needed home workers had them, but these were often limited to specific roles, or levels – such as the need to work in the evenings or weekends – and could only access limited data and resources. For the rest of the workforce to work from home, solutions needed to be put in place to facilitate this.

The number of home working and mobility solutions on the market is staggering. Without these solutions the workforce could not have adapted as quickly as it did. But with that speed of change, there are always a few teething problems. In many cases, businesses have failed to consider the limiting factors that pose serious security risks. Perhaps the biggest concern of all is the flaws in human behaviour.

Behavioural concerns:

The sight factor	Staff that are not supervised directly, with line of sight, will be less productive.
The 'empire' factor	Management enjoys being able to physically see, and be in control of, their employees.
The morale factor	Teams function better with regular face-to-face interaction, including professional and the more social water-cooler chats.
The office factor	People work in offices, but get distracted at home.
The reluctance factor	People are averse to change, particularly in organisations that have always worked in the same way.

In addition to the human factors, businesses had also failed to consider the home working limitations created by compliance and regulatory considerations. For many, working from home was a completely new experience – and so were the technology issues it produced.

Both the technology concerns and behavioural factors have impeded the adoption of home working for a number of years. Businesses have been reluctant to let employees stay at home for fear that productivity will fall – yet, when forced to do so, 28% of UK employers found productivity and efficiency had both increased.[4] But not all of these factors are so easily overcome.

Technology concerns:

The data factor	All data is a commodity that can be exploited. If workers can access it from home, others can too.
The performance factor	All workstations won't necessarily be able to work in the same way – performance issues from inconsistent internet connections to failing to update software will affect productivity.
The compliance factor	All employees are subject to regulations, such as the Payment Card Industry Data Security Standard (PCI DSS), no matter where they conduct that business.

Consider home workers that don't have a dedicated set up, such as those working at the kitchen table. This could be a significant security risk. Who else can see what's on their screen? Would you want your employees' family members or housemates seeing confidential information such as financial records, health data or payment card information?

As well as breaking company rules, this could be a breach of regulations like GDPR and the Payment Card Industry Data Security Standard (PCI DSS).

And what about customer service? It isn't just unreliable internet connections that could pose a problem. Poor performance from background noise, call drops and inaccessible applications could all impact the experience of customers.

There has long been an increasing demand for more flexible working patterns. And if it works, it's a win-win for employers and their employees. Flexibility works both ways, employees can have more control of their hours and employers can meet fluctuating demand in more imaginative ways. In the future, call centres may be able to respond to a peak in calls by issuing an alert and employees could log in within minutes to help out for the time needed.

This is the future. Making changes now will set you up for that future. But it isn't just about finding solutions that allow you to connect your office to homes, it's about deploying additional measures to help employees do their jobs effectively and safely.

Securing customers' information

Dual-Tone Multi-Frequency (DTMF) masking is one way businesses can protect customers' sensitive information from outsider threats like hackers, and insider threats like rogue agents trying their luck.

DTMF tones are the beeps generated when a user presses the keys on their phone. Instead of asking the caller to read out details for identification or validation – such as their card number or date of birth – the agent will ask the customer to enter them using the keypad. The DTMF masking system will intercept the distinctive tones and convert them into data to be processed, meanwhile muting them from the agent. The system is then able to verify the details without them being exposed to the agent. The experience is seamless for the caller and the risk of data compromise is dramatically reduced.

COVID-19: A game changer

Things may never be the same again.

Where before companies were considering adapting to home working and exploring how to make it possible, COVID-19 gave businesses no choice.

Rapid decisions had to be made, often to prevent businesses suffering dramatic losses – the existence of the business itself depended on quick decision making. The rapidity of these decisions meant that the normal due diligence was not in place when they were taken. Security and compliance staff were often not consulted in the decision to send staff home to work, or if they were, they did not have time to assess the situation in detail.

So this is where many businesses find themselves today, they now have, and will continue to have, far more home workers than ever before. Even once businesses can return to their usual places of work, almost three-quarters of employees said they wanted a hybrid form of working – working from home some of the time and at least one other location the rest – if given the choice.[5] It seems as though working five days a week in the office has become a little old-fashioned.[6]

Employees want to be, and will need to be, mobile. That's great news in terms of recruitment – the talent pool is now global instead of local. Businesses can recruit from anywhere and get agents up and running in next to no time. And with costs reduced – as less dedicated office spaces are no longer required – this could result in significant long-term savings.

But this shift will present new security challenges. Companies will need to plan for and effectively manage the use of personal devices – many already do with bring your own device (BYOD) policies. And they will have to update policies to address workspaces in the home, including not just cybersecurity, but physical security too.

Flexibility for everyone

Employees have the right to a work-life balance. And in many countries – such as the UK and all members of the European Union (EU) – that right is enshrined in law. As part of that they can request flexible working from their employer. These requests must be considered, and if the employer denies the request they must provide a good reason for doing so. With so many workers having been working from home for much of 2020 and beyond, it's going to be hard for employers to deny such requests in the future.

Home, hybrid or office: A global breakdown of working location preferences

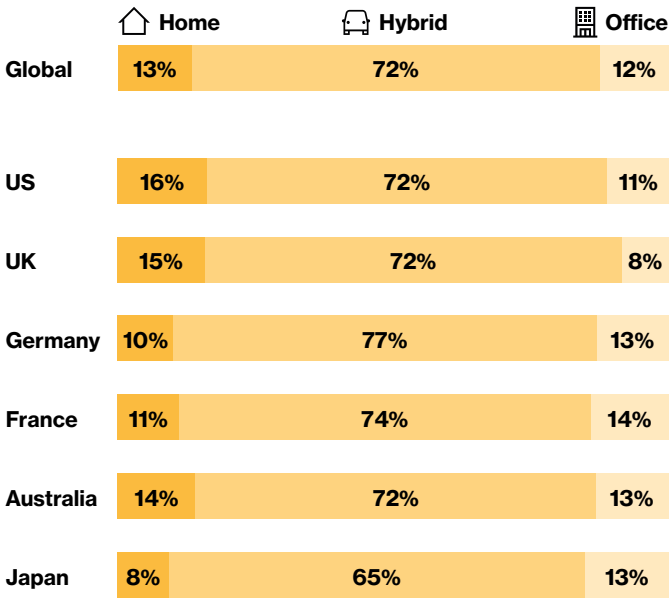


Figure 1: Home, hybrid or office?: A global breakdown of working location preferences. Totals may not add up to 100% due to "don't know" responses, which have been omitted.[7]

Prepare your staff for home working.

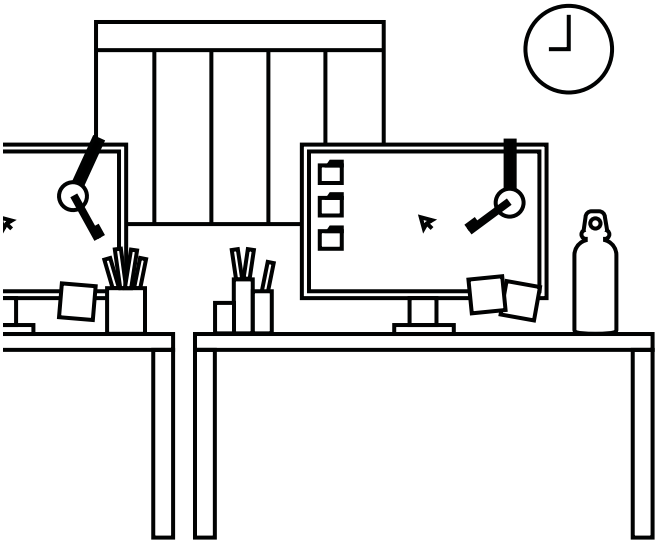
Businesses now have the opportunity to make working from home a safe and viable future option for their employees. The first thing to consider is the effect working from home may have on your employees themselves. It's a daunting prospect to start working from home for people who haven't done it before. It's even harder when they're just thrust into it. Not everyone will be OK with suddenly working remotely on their own.

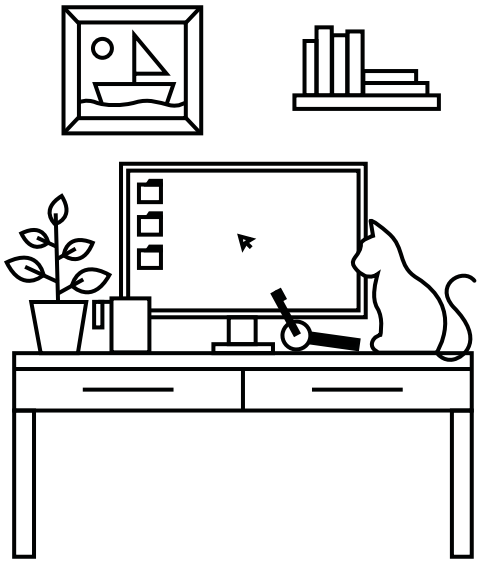
Make the transitions easier and help keep your employees connected. During the COVID-19 pandemic there was a huge surge in downloads for video conferencing apps as businesses focused on providing employees with tools to stay connected. But as we move forward, think about whether you have appropriate services in place – like chat rooms, video conferencing and document sharing – so that teams can continue to collaborate.

Recreating the team environment of the traditional office space, albeit virtually, can help you monitor how your staff are coping and identify any dips in morale. These conferencing tools don't just enable staff to continue serving customers, they can also be used to check in on one and other to avoid feelings of isolation. Keeping an eye on employees' wellbeing can help you maintain morale, which in turn can drive productivity – and help reduce errors.

Your staff might feel more exposed to cyber threats when working outside the office environment. Then on the other hand, employees may suffer from a case of "out of sight, out of mind". Without an IT team or management physically alerting them to security policies and issues, employees can fail to grasp the seriousness and inadvertently put themselves, their business and its customers at risk.

Now is the time to re-educate your employees and explain why cybersecurity is something they should all care about. There are lots of great tools out there for you to take advantage of, like the National Cyber Security Centre's (NCSC's) Top Tips for Staff e-learning package. Working with key partners too can help. Verizon's security consultants can help you identify security gaps, enhance the visibility of risks and evaluate where you need to focus. That focus can help your security team understand which elements of your security posture are most vulnerable and where to prioritise for remediation.





The threats facing home workers

As employees move from the office to home, they'll be making more use of mobile devices – that's not just limited to mobile phones, it includes things like laptops too. These types of devices are a prime target for cybercriminals. Regardless of where these devices are used, the threats – phishing, ransomware and malware to name a few – and their consequences remain the same. When most people think of cybersecurity compromises, they instantly think of loss of data. While that is a factor, it's not the only one.

Consequences of compromise.

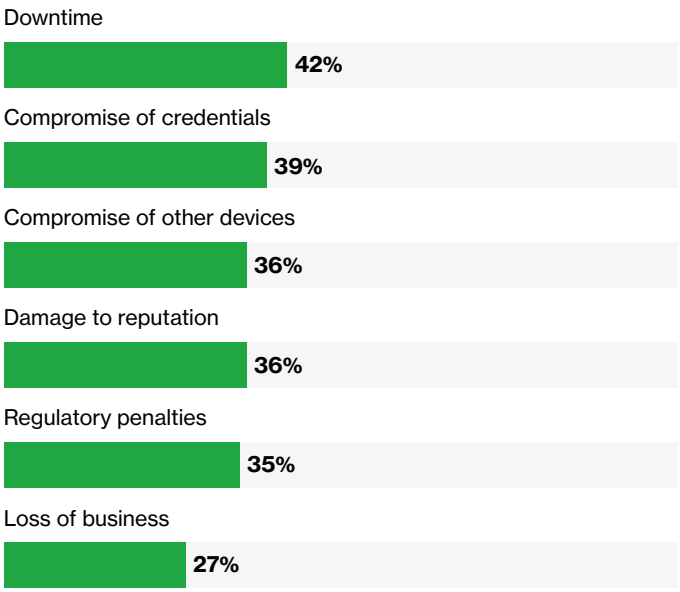


Figure 3: Which of the following consequences did your organisation experience as a result of that [mobile-related] security compromise?[8]

In fact, the majority of companies experienced downtime as the biggest consequence of a mobile security compromise.[9] That's an even bigger problem now the workforce is so dispersed. With employees not in one central location it can be much harder to get everyone up and running again. Any time lost to remediating a compromise is time that businesses aren't serving their customers.

It's important that businesses put the correct measures in place as remediating a mobile breach can be costly and have lasting repercussions. The effect on your reputation can be one such repercussion that not all businesses bounce back from. Plus, failing to keep up with customers' increasing demands can have a significant impact on customer satisfaction scores (CSAT) – it's hard enough with the way workplaces have been disrupted recently, don't let your security, or lack of, be another barrier in the way of serving your customers.

Dealing with a security compromise

How not to do it

There are many examples of organisations that didn't deal with security compromises and data breaches in a way that satisfied customers, employees, investors or regulators.

In 2016 the information of 57 million riders of a well-known ride share platform was compromised. But the company didn't disclose this until 2017. Instead of alerting users, it decided to try and cover up the breach.

This ploy resulted in a US$148 million settlement and the CSO spending more time with his family. The company's reputation was badly affected and calls to boycott it became a trending term on social media.

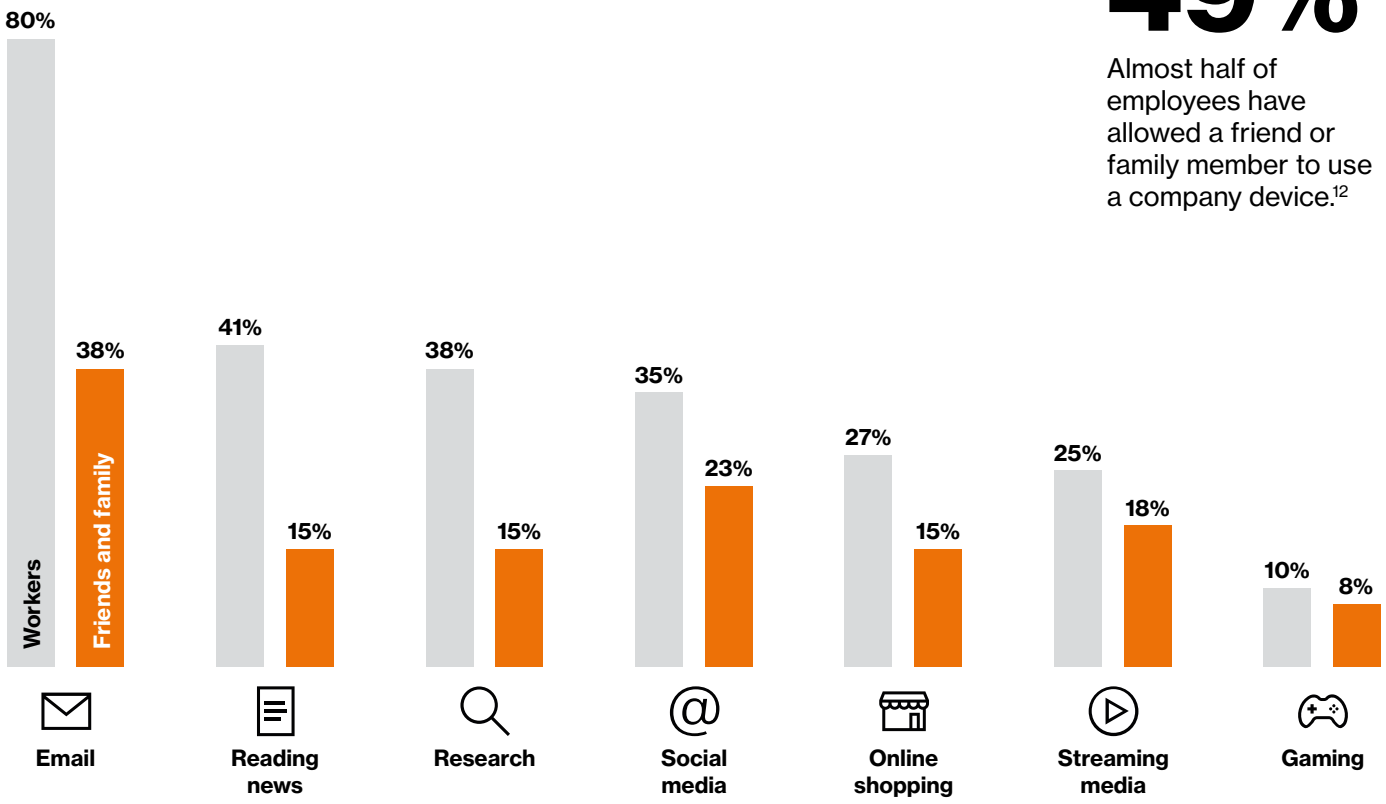
How to do it properly

Unfortunately breaches can happen to anyone, and if they do happen to you, it's how you respond that matters. Some organisations have done it right.

A graphic design start-up showed how responding quickly and maintaining transparency with customers at all times is key.

Once it was made aware of a security compromise in May 2019, its first response was to lock down its app. Straightaway, mid-attack. It then notified users and the authorities of the compromise. It gave users frequent updates and continued to do so for over a year after the incident. This response has helped to establish the company as one that is doing its utmost to protect its users and their data.

It's not just employees using company devices for personal tasks.



49%

Almost half of employees have allowed a friend or family member to use a company device.[12]

Figure 4: Percentage of workers who use (or permit the use) of company devices for personal tasks.[10]

Avoiding bad habits

Perhaps the biggest mistake employees are making is falling for phishing. These attacks are more sophisticated than ever before, and will often prey on real-world concerns. The COVID-19 pandemic has spawned its fair share of scams claiming to have a 'cure' for the virus or encouraging you to donate to help others. Phishing attacks will use whatever it takes to get users to click, and once they do click it doesn't take much for malware to be downloaded onto their device.

Not quite as scary as phishing, but no less serious, is employees using devices for personal tasks. Though many companies have policies in place to allow some level of this, employees are still accessing things they shouldn't be. Things like answering personal emails may be allowed within an acceptable use policy (AUP), but accessing adult, extreme, illegal or gambling content on company devices is clearly unacceptable. It isn't just about the effect it could have on the businesses' reputation, these sites are often rife with malware and malicious threats. With employees at home there is less control of this – particularly as 49% have let friends or family use work devices for personal tasks too.[11] They certainly won't have read the company's AUP.

More important than what they're accessing, is how they're accessing it. Employees are using their own internet connections – do they have the correct levels of security in place? How many still haven't changed the default password on their routers? These are important things that need addressing to keep employees and the wider business secure.

Employees, especially those working from home for the first time, are often going to lack the skills and knowledge to operate safely. One way to reduce the risk is to reduce the amount of data they have access to. Introducing strict "need to know" data management policies is a key step. There is also DTMF masking (see page 5), that can reduce the amount of sensitive information that is exposed to the agents.

Security shouldn't put in so much red tape that agents look for ways to cut corners, you need to help them to make smart decisions.

In the next section you'll find recommendations to help all of your home workers improve their security knowledge and better protect your business. We've broken home workers down into three different categories: Established, Emerging and Exigent.

Recommendations for safer home working

The following table gives recommended actions to increase security and protect your business and customers, broken down into three categories of home workers.

Users and behaviours

Common threats

Social engineering, phishing, business email compromises (BEC), policy breaches and inappropriate usage

All

Remember, many of your staff are already stressed, so they're not in an ideal position to learn new technologies. So take your time and consider introducing changes to behaviours and mindsets first.

You should check how staff are coping; not just in terms of how to use new technologies, but also how they are adapting to having to work in very different ways. Tired, and despondent employees are more likely to make mistakes.

In addition, they might not be able to ask an office workmate for help, as they normally would. This makes them more vulnerable to attacks like social engineering and phishing, where fraudulent attempts exploit staff to obtain information and enticing links become gateways to malware.

Educate your employees to be on the lookout for these attacks and other suspicious behaviour and to never divulge information without verifying the request.

Where applicable, give your employees training with attack simulations. At the very least teach them how to spot the signs of phishing – things like checking the email address it was sent from, and the URL it's trying to send you to. Misspelled addresses are often a big giveaway.

Don't just limit your training and policies to emails and laptops – mobiles, SMS, IM apps, social media and games are all targets too.

Make sure all staff know how to report any problems. And that you have a clear incident response plan in place. Failing to do so could cause more issues further down the line.

Ensure that all policies are up to date, and that you have relevant ones in place such as a clear home working policy and a clear AUP. Provide training and give regular updates to help staff follow these policies.

Ensure staff understand the importance of keeping software (and the devices themselves) up to date, and that they know how to do this.

Depending on the experience of your staff (and the applications you provide), you should consider producing a series of 'How do I?' guides so that your already stretched support team isn't overwhelmed with requests for help. For example, you might produce a 'How to log into and use an online collaboration tool' guide.

Established

Many organisations have already introduced this training for home-based workers, but not all, check if this is the case with your company.

Staff in the Established group should be familiar with these processes, however, it may be appropriate to run a refresher course online, especially in response to the increased fraud rate as a result of COVID-19.

Emerging

Many organisations have already introduced this training for home-based workers, but not all, check if this is the case with your company.

In the case of the Emerging group, it is good to check they have received such training, as this may have been overlooked in the rush to get staff working from home.

Staff may require the introduction of new content to existing policies to cover their new found home-based role.

Exigent

It is good to check that staff have received such training, as this may have been overlooked in the rush to get them working from home.

Staff in the Exigent group are the most likely group to have not been trained in security and may not be familiar with these processes (particularly the home worker policy).

Even if they are, it may be appropriate to run a refresher course online, especially in response to the increased fraud rate as a result of COVID-19.

Staff may require the introduction of new content to existing policies to cover their new-found home-based role.

Established

Employees that have been working from home for some time and are well versed in what's involved. This includes "Omniworkers" that mix home working and going into the office.

This group normally presents a lower risk to the business as the technology is well established. But this can be higher if training and processes are inadequate.

Emerging

Workers performing similar duties to those in the Established group, not previously allowed to work from home. Typically this was due to the human-factor reasons discussed above – such as concerns about supervision and productivity. However, the available technology is perfectly capable for their use.

This group often presents a somewhat higher risk to the business as they may not be familiar with processes and best practices.

Exigent

Those now working from home despite their role not really being suitable for being done outside of the office. These are the roles above the traditional home working technology market penetration point; ones that home-working technologies were not designed for. These employees are only home-based for an extenuating reason, such as COVID-19.

These roles typically present the highest risk to an organisation.

Apps

Common threats

Malware, out-of-date apps, leaky apps, password snooping, overzealous permissions.

All

Remember that all employees will still need access to a variety of apps to do their jobs – perhaps even more so when working remotely.

You can limit employees' use of apps to the bare minimum required, but that can have negative effects on morale and lead to inappropriate downloading of unapproved apps.

Instead, introduce an AUP and encourage good habits.

Make sure your organisation has a patch policy. Ensure all employees are updating apps on all of their devices when they are required to do so.

Consider something like cloud access security broker (CASB) that won't let you connect to company web apps if your device doesn't meet set security standards, including patches.

Remote users may need to use different software (or use familiar applications in a different way) compared to what they do when in the office. You should produce written guides for these features, and test that the software works as described.

If you need to set up new accounts or accesses so your staff can work from home, you should set strong passwords for user accounts. Please refer to the NCSC guidance for system owners responsible for determining password policy. The NCSC strongly recommends you implement two-factor authentication (2FA) whenever available.

Where applicable, ensure staff are backing up their devices so that if any downtime should occur you can get up and running again as quickly as possible.

Teach staff to look out for and report suspicious or unexpected system behaviour. Something like a device constantly needing charging might be seen as just an annoyance, but could actually be an indicator of a malware compromise.

Monitor devices for unusual behaviour – including excessive data transfer and out-of-hours use – that could indicate that an application has been compromised.

Established

Staff in the Established group should be used to this process.

Emerging

Staff in the Emerging group should be used to this process but may have relied on others to remind them about updates.

Exigent

Staff in the Exigent group may be aware of this process but would have relied on others reminding them about updates.

They will also be accustomed to an IT team restricting their usage and access to apps – this may not always be possible when working from home.

Appropriate training needs to be given to ensure staff know how to use apps correctly and how to set them up securely – such as limiting permissions to things like your camera and microphone when it isn't required.

Devices

Common threats

Out-of-date operating systems and lost or stolen devices.

All

Remember that employees are just getting used to using a plethora of new devices. Going mobile may be a first for some, and so will be using these devices for work purposes.

Devices used for working outside an office environment are more vulnerable to theft and damage. Whether using their own device or the organisation's, encourage staff to lock their screens if left unattended, especially if there are children or housemates present. When the device is not being used, staff should keep it somewhere safe.

Staff are more likely to have their devices stolen (or lose them) when they are away from the office or home. Make sure devices encrypt data whilst at rest, which will protect data on the device if it is lost or stolen. Most modern devices have encryption built in, but encryption may still need to be turned on and configured.

Make sure that staff know what to do if their device is lost or stolen, such as who to report it to. Encourage users (in a positive, blame-free manner) to report any losses as soon as possible. The early reporting of such losses may help minimise the risk to the data, and staff who fear reprisals are less likely to report promptly.

Fortunately, the majority of devices include tools that can be used to remotely lock access to the device, erase the data stored on it, or retrieve a backup of this data. You can use mobile device management (MDM) software to set up devices with a standard configuration.

Think about the specifics of being at home. If you have a BYOD/BYOPC program, you might not ever get to physically touch the device. Make sure you have policies in place and provide employees with adequate training to take the correct security measures.

USB drives can contain lots of sensitive information, are easily misplaced, and when inserted into your IT systems can introduce malware. When USB drives and cards are openly shared, it becomes hard to track what they contain, where they've been, and who has used them.

You can reduce the likelihood of infection by:

- Disabling removable media using MDM settings
- Using antivirus tools where appropriate
- Only allowing products supplied by the organisation to be used
- Protecting data at rest (encrypt) on removable media

Lots of companies block file sharing internally, but this simply isn't an option when working from home. Staff need to collaborate and work on files simultaneously. Give them an approved way to do this safely and you're less likely to encounter problems.

As with apps, ensure that staff are keeping the operating systems of all their devices up to date, failing to do so could put your whole business at risk – not just the compromised device.

Remember that some updates can only be done when plugged in and on Wi-Fi. Make sure to remind employees to set aside time and prioritise getting these done.

Established

Staff in the Established group should already be very familiar with these processes and should have developed good habits.

Emerging

Staff in the Emerging group may not be used to this process as office based workers often leave their machines on all of the time. They will need further training to understand the importance of this risk.

In the rush to get workers set up at home you may have bought a whole load of new devices quickly, or even implemented BYOD at speed. As a result you may not have been able to give staff the appropriate training for how to use and look after each device.

Provide training, and where possible write guides that can be used to refresh staff's memories without providing a further burden on your overstretched support teams.

Exigent

Staff in the Exigent group may not be used to this process as office based workers often leave their machines on all of the time.

In the rush to get workers set up at home you may have bought a whole load of new devices quickly, or even implemented BYOD at speed. As a result you may not have been able to give staff the appropriate training for how to use and look after each device.

Provide training, and where possible write guides that can be used to refresh staff's memories without providing a further burden on your overstretched support teams.

Networks and cloud

Common threats

Insecure networks, rogue Wi-Fi and man-in-the-middle attacks.

All

Remember some employees will be working from home for the first time so may not have the appropriate precautions in place on their home network solutions.

Conduct a network security evaluation. Speak to your communication provider about the best way to test the security of your communications environment, evaluate your organisation's work practices and staff training. Work with them to determine your security requirements – for example the use of Virtual Private Networks (VPNs) and encryption.

VPNs allow remote users to securely access your organisation's IT resources, such as email and file services. VPNs create an encrypted network connection that authenticates the user and/or device, and encrypts data in transit between the user and your services. If you are already using a VPN, make sure it is fully patched. Additional licenses, capacity or bandwidth may be required if your organisation normally has a limited number of remote users.

At a fundamental level, ensure staff are connecting their work devices to secured networks. Restrict, and limit altogether if possible, the use of public Wi-Fi for any work devices or work-related tasks. This includes Wi-Fi hotspots, even those of well-known brands, as they too cannot be fully trusted.

Update, or introduce, policies to cover different networks and what functions should and shouldn't be performed on them. Clear guidance will help your employees make smart decisions and connect securely, even when out and about.

Ensure all employees have taken the security measures they can with their home Wi-Fi including changing the default password and limiting the access to other trusted users.

Established

For existing home workers this is a step that has usually been done, but it is always good to check and get up-to-date advice. This may not be the case in the other user types if they have been deployed rapidly. Do not assume if your organisation has added home workers that they are all working using the same technologies.

Emerging

If home workers have been deployed rapidly as a response to COVID-19, they may not be using the same technology as existing home workers. Do not assume they are all working using the same technologies.

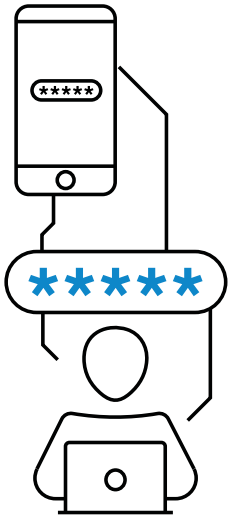
Exigent

Do not assume all home workers are using the same technologies – those that have been deployed rapidly, may not be.

This group may need additional tech – for example if they take credit card payments over the phone additional software may be required to comply with PCI DSS regulations. Examples of this may be DTMF suppression software. This may have been overlooked at the time of deployment and may be required.

An employee's guide to working from home safely

verizon



Reduce risky behaviour

Make sure you read and understand your company's policies. Ask for further guidance if there is anything you're unsure of. These policies are in place to protect you and the company, it's important you follow them.

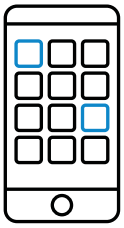
Remember to try and keep your private and work life separate. It can be difficult to do, but it's important both from a mental wellbeing and security point of view. If the kids' school account needs topping up with dinner money, or that eBay auction is close to ending, use a personal device, not a company one.

Consider where you keep work devices and any confidential data. Make sure that you've set a password or PIN – or enabled Touch ID or Face ID where applicable – for access. Set up the device to lock automatically after a few minutes of inactivity. Where possible, set up "hot corners" or a "hot key" to quickly lock the device if you need to step away. If you're leaving the house or will be away for an extended period, put the device out of sight.

Create strong passwords for all accounts and web applications. It's advice that you'll have heard before, but it's more important than ever. Turn on two-factor authentication wherever possible.

Think about who can see or hear what you are saying or typing on your screen. Could a housemate or somebody doing work in your home look over your shoulder? Or do you work with the windows open in the summer? Any of these could lead to sensitive data being inadvertently shared.

Sign up to newsletters from trusted organisations, such as the NCSC's weekly advisory. Knowing your enemy is the first step to defeating them. Plus, you'll be able to share that knowledge with your colleagues, and cybersecurity skills are always in high demand.



Manage your apps

Be careful what apps you install on your devices, especially when that device has access to corporate resources. Make sure you're clued up on your company's acceptable use policy (AUP) and any other restrictions that may be in place.

Installing updates can be a bother, but resist the urge to tap the "snooze" button. Repeatedly postponing updates could put your device, and the whole company, at serious risk.

Watch for apps asking for lots of permissions and give permission sparingly. A lot of apps will ask for access to your camera or microphone when it's not strictly necessary. Don't just select "Allow all", actually go through and reject any that are not needed. Consult your company's policies for further advice on what to limit on what apps.

Secure your devices

Don't share devices. You may be allowed to perform personal tasks on your work devices as set out in the AUP, but that doesn't apply to your friends and family. No matter how much you trust them, something as simple as them checking their social media feed could be enough to lead to a serious security risk or the compromising of your company's sensitive data.

As with apps, install operating systems updates when asked to do so. Remember some devices will have restrictions on when updates are installed – such as the device being plugged in and on Wi-Fi (not cellular).

Look after your device. But if you do lose it, or it gets stolen – these things happen – report it immediately. That way your company can protect the data it holds, such as credentials for accessing key systems, by locking the device or performing a remote wipe. Although you might be tempted to wait and see if the device turns up, this will only make things worse.

Be smart about networks

Chances are you haven't changed the default password on your home Wi-Fi. Make sure to do this as soon as possible. If you are not sure how to do this, your internet provider should be able to tell you how, or there are plenty of free guides online to help.

Think about what else you attach to your home network – doorbells, camera, other personal mobile devices. Check that these are all running on the most up to date software and you install any new patches promptly. Make sure these devices have the appropriate security settings in place – it's a good idea to change the default passwords on these too.

If your company provides a Virtual Private Network (VPN), use it. Your company should give you all the information and should help you set this up.

Be really careful of public Wi-Fi networks. Even one associated with a brand you know and trust could be insecure or harbour malicious code. Avoid using them for any work-related tasks wherever possible.

Conclusion

Working from home has already become the norm. Whether it's something all employees do, or just those that need to; every day, or just several times a week, it's something all businesses need to make a fully viable long-term option.

We may have all been doing it during the COVID-19 pandemic, but that doesn't mean we're doing it as well as we could be. Before rapid decisions had to be made to avoid disruption to business and continuing to serve customers was the priority. Now that priority needs to be protecting customers.

Verizon has the experience to help you understand the threats your home workers are facing. Knowing the different types of threats is the first hurdle, then we can focus on overcoming them. There are solutions out there for every business, and we can help you find the right one for you. Don't disrupt your operations any further, it's time to give employees the training and support to work from home effectively and implement the right solutions to protect them further. You don't have to face this alone.

Expand your knowledge

Learn more about the threats with Verizon's range of security publications.

Mobile Security Index 2021

Mobile connectivity transformed the way we work before the COVID-19 pandemic, and has long been a prime target for cybercriminals. Now in its fourth edition, this report will help you understand the threats facing your mobile devices and learn how to mitigate them and protect your business.

Data Breach Investigations Report 2020

Learn from real examples and stay ahead of threats with insights from 3,950 confirmed data breaches. Get the information you need to put improving your security at the top of the agenda.

Insider Threat Report

Not all threats come from the outside. Insider threats, perpetrated by employees, contractors, interns and leaders within an organisation are real and can quickly destroy businesses. Learn how to defend against them.

Verizon's CX services

Contact Center and CX Solutions

Verizon's Contact Center and CX solutions can help you to continue to deliver the same great service your customers know and expect – from wherever you are. With cloud, virtual and unified options there's something to suit every business.

Find out about our other CX services >

Virtual Agents

Employ Verizon's Virtual Agents, powered by artificial intelligence, to make great first impressions with your customers and relieve the burden from your employees.

PCI Advisory Service

Navigating the ever changing financial regulations and security requirements can be a headache for your business. Our solutions can help take the burden off your hands so you can better serve, and protect, your customers.

Find out about our other security services >

Application Performance Management and Monitoring

Give people the seamless experience they expect. Manage and monitor your apps to gain full visibility across your network. Respond and adapt quickly to business challenges and boost your security.

References

1 TUC, Growth in homeworking has stalled, 18 May 2018

2 CIPD, Home working set to more than double compared to pre-pandemic levels once crisis is over, 16 July 2020

3 Verizon, Mobile Security Index, April 2021

4 CIPD, Home working set to more than double compared to pre-pandemic levels once crisis is over, 16 July 2020

5 Slack, Moving beyond remote: Workplace transformation in the wake of Covid-19, 7 October 2020

6 Reuters, REUTERS NEXT-Unilever 'strongly encourages' workers to get COVID vaccine, 13 January 2021

7 Slack, Moving beyond remote: Workplace transformation in the wake of Covid-19, 7 October 2020

8 Verizon, Mobile Security Index, April 2021

9 Verizon, Mobile Security Index, April 2021

10 Proofpoint, State of the Phish, January 2020

11 Proofpoint, State of the Phish, January 2020

12 Proofpoint, State of the Phish, January 2020

verizon