CyberSmart

CYBER SAFETY IN A NEW ERA OF WORK

HOW TO MAKE THE SAFE SWITCH TO PERMANENT HYBRID WORKING

Click to download

020 7993 6990
hello@cybersmart.co.uk
www.cybersmart.co.uk

CONTENTS

WELCOME TO CYBERSMART

Built for SMEs with limited cyber expertise, CyberSmart offers you a simple, step-by-step journey to securing your business.

In this e-book we show you how to protect your business from the threats posed by the future of remote work.

www.cybersmart.co.uk

The transition to permanent remote working has begun

Unless you've spent the last few months consciously avoiding the media, chances are you've read that sentence a lot. From morning talk shows to breathless newspaper op-eds, it feels like everyone is talking about the society-wide shift to working from home.

But what started as a necessity that many businesses adopted reluctantly has transformed. First came announcements from Twitter and Facebook that employees would be allowed to 'work from home forever' if they chose. This was followed by a host of other businesses including Google, Amazon, JPMorgan, Capital One, Slack, Salesforce, Microsoft and PayPal extending their work-from-home options.

This switch towards remote working isn't just the preserve of globe-striding corporations either. 43% of UK SMEs made the jump to remote working, within a week of lockdown measures being implemented in Britain.

Why is this happening?

Well, it's actually very simple. An increasing number of businesses are seeing the real benefits of a more permanent shift to remote working. Why rent office space for 300 people when you could use a smaller venue for essential meetings at half the cost? Why insist staff make long commutes into the office, when they're happier and more productive working from home?

For many organisations, the COVID-19 pandemic has turned these questions from water cooler conversations into key pillars of business strategy. And, although the jury is still out on some of the benefits of remote working, early indicators are positive. According to a recent survey from Intermedia, 57% of SME owners said they are likely to increase remote working options for employees in the long term. Some of the reasons cited for this include increased employee availability (19%) and life satisfaction (7%) and reduced overhead costs.

It's fast becoming clear that remote working is no longer a 'nice-to-have' or the terrain of millennial-led startups – it's a viable option for small businesses in every sector. But like any new approach, working from home brings with it fresh challenges, particularly in the realm of cybersecurity. So if your business is considering making the switch to permanent remote working, there are some risks you need to be aware of. Let's take a look at some of them and what you can do to overcome them and ensure your business and people are safe.

> 57% of SME owners said they are likely to increase remote working in the long term.

05

What are the risks of working from home?

While switching to remote working offers benefits in productivity and real estate savings, it also comes with some risks.

Here are a few of the most common.

Unsecured personal devices
The first question to ask is: can you be sure your people will follow the same security protocols they would in the office? The networks and security tools your staff use at home are likely to be far less secure than those in the office. Home office networks are 3.5 times more likely than corporate networks to be infected by malware, according to a report from BitSight. There may even be a psychological element to this. As ZDNet has reported, 52% of employees believe they can get away with riskier behaviour when working from home. For example, sharing confidential files via email instead of the usual, safer channels.

Lack of remote-working policies and procedures
Part of the reason employees are exposing themselves to risk at home is simply a lack of knowledge of these risks. The COVID-19 pandemic developed so quickly that many businesses didn't have time to put in place clear policies and procedures for working from home so employees were literally left to their own devices.This makes cybersecurity a bit of a guessing game, particularly for the less security-literate of your staff.

06

Risks of working from home

Heightened risk of attack

Cybercriminals are smart but they're largely opportunistic. And it hasn't taken them long to figure out that switching to remote working has made businesses vulnerable. VMWare's recent Global Threat Report, reveals that 91% of global respondents have seen an increase in cyber attacks as a result of employees working from home. Meanwhile, the proportion of attacks targeting remote workers increased from 12% of all email traffic in March to 60% just six weeks later.

Keen to exploit our hunger for coronavirus updates, cybercriminals have set up thousands of COVID-19-related 'news' sites. These double up as hosts for malware and domain names to launch phishing attacks from. Without the robust controls deployed by most corporate networks, it's incredibly easy for people working from home to fall into the trap.

The other area cybercriminals are targeting more regularly is VPNs. VPNs have long been a weak point for cybersecurity. They were only ever intended for small numbers of workers to use occasionally, not whole companies all the time. As a result, many VPNs are insecure and provide cybercriminals with a much wider 'attack surface' with which to launch threats.

> 91% of organisations have seen an increase in cyber attacks as a result of employees working from home.

Risks of working from home

Reliance on the Cloud

While using cloud storage is the safest option for most businesses, it's not invulnerable to attack. Working from home naturally increases your reliance on the Cloud. And this isn't necessarily a bad thing. However, cybercriminals are becoming better all the time at breaking through providers' defences and intercepting data as it moves between employees' devices and the cloud.

Data protection

What about GDPR? Of course, working from home doesn't mean that the rules of GDPR don't apply. But unfortunately, some of the risks we've already mentioned – such as insecure devices and unclear or non-existent policies – make a breach more likely.

To illustrate, what makes for any easier target? A physical workplace in which everyone follows the same cyber hygiene rules and uses one well-protected network. Or a team of employees across a geographic spread, each with differing levels of home security and, if we're honest, adherence to policies. Cybercriminals know this, which is why employee devices and unsecured home networks are becoming such a tempting target.

How to overcome the risks

We've tackled some of the risks involved in switching to working from home, so what can you do about it?

Provide clear policies and encourage communication

This is the most important step on this list. If your people don't know which behaviours are harmful, they can't correct them. Ensure all security policies for workers are clear and easy to follow. If you don't have a remote working security policy, now's the time to draft one. Alongside this, work to foster a culture of communication. That way, employees will feel comfortable asking for help with anything they don't understand and reporting anything suspicious to internal security teams. All too often, security mistakes are made because staff feel 'silly' raising their concerns.

Ensure the right security is in place

Many of the most common threats can be prevented simply by ensuring your people have the tools they need. Check that all corporate-owned or managed devices are equipped with the best security capabilities. Also, make sure that the security best practices you'd use in the office are extended to the home environment.

Maintain good password hygiene

Set up a password policy and ensure everyone follows it. Employees should always use complex and different passwords, and two-factor authentication when possible.

Overcoming the risks

Make sure software is up to date
Your employees should regularly install updates and patches for the software on their devices, no matter how much they might enjoy not restarting their laptop for months on end.

Keep it professional
Encourage your workers to keep work devices for work and personal devices for everything else. Limiting the number of sites employees visit can limit the risk of attack.

Secure Wi-Fi access points
Network gateways are an under-appreciated aspect of good cyber hygiene. Most of us don't think much about our WiFi once it's up and running. However, changing the default settings and passwords on a router can reduce the potential of attack from connected devices.

Get Cyber Essentials certified
According to a report from Lancaster University, the measures laid out by the UK government's Cyber Essentials (CE) scheme can mitigate 98.5% of cybersecurity risks. If you're not already CE certified, following the process will help you build a great base level of security for shifting to remote working.

> The UK government's Cyber Essentials (CE) scheme can mitigate 99% of cybersecurity risks.

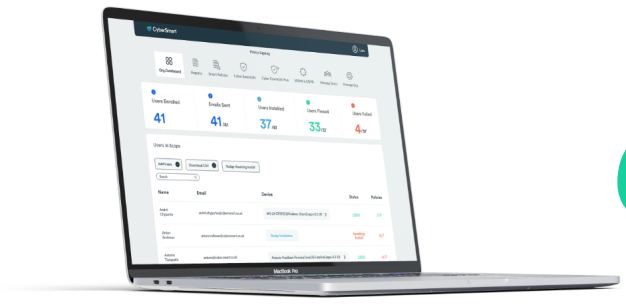
Simple protection with CyberSmart

Although, all of the options we've discussed so far will help you reduce the risks presented by working remotely, they can be tricky and time-consuming if tackled individually. But there is another way.

The CyberSmart platform guides you through a simple step-by-step journey to becoming cyber secure. It starts with assessing how you're currently doing, and guides you all the way through to achieving security your customers can trust. You can even complete Cyber Essentials certifications in-app – whether it's your first time or you need to renew an existing certification.

But CyberSmart doesn't just make your small business cyber secure, it keeps it that way. CyberSmart monitors all of your company devices 24/7 checking for the most up-to-date applications, operating systems, firewalls and security measures. What's more, CyberSmart helps improve staff understanding and engagement with cybersecurity. We make security policies shareable across all company devices and check who's read them. CyberSmart provides everything you need to get cyber secure, with no requirement for cyber expertise or expensive technology.

The switch to working from home comes with difficulties, but it's also a golden opportunity to remould the way your business functions. Alongside the obvious real estate savings, remote working promises happier employees, more productive work and greener business practices. Don't let poor cybersecurity stand in the way of your business embracing the future.



> CyberSmart prevents up to 98.5%* of all cybersecurity incidents.

CyberSmart

CyberSmart provided us with a fantastic experience. Their automated app makes managing and keeping compliant with Cyber Essentials very easy. To get us certified, their team went the extra mile and helped us effectively with their simple and straight forward process. So I highly recommend using them if you want to get your cyber essentials certification in a trouble free method.

- Zein S.

Trustpilot

Get in touch

68 Hanbury Street
London
E1 5JL

020 7993 6990
hello@cybersmart.co.uk

www.cybersmart.co.uk