MODERN WORKPLACE

Into the era of secure remote work

A business guide to cloud security for the new remote workplace

cmi

Microsoft 365

Business opportunities and security risks associated with the rapid shift to remote work

Something many small and medium-sized businesses have discovered during the rapid shift to remote everything: There's a lot to be gained by not relying on a physical space. It can save overhead, reduce travel expense and some studies have found it has increased worker productivity (one found a 13% performance boost among at-home workers).[1] As a result, many businesses are seriously considering tools and strategies to make the non-physical workplace a permanent part of their businesses.

To succeed, this transformation of physical businesses will require new structures and processes, especially for smaller businesses that were not used to working remotely. Regardless of size, all companies now need to think about securing remote endpoints and IT resources. Employees need to be more vigilant than ever. Cyber attackers have made it clear they're not taking any time off.

Many of us saw the additional security risks of the remote work explosion. Video data breaches represent only the visible fraction of other, less flamboyant, but more costly threats enabled by the new scale of endpoint devices in use. Over just a single initial month of the crisis, the National Cyber Crime Security Centre detected:

- **555 malware distribution sites** set up to cause significant damage to visitors
- **200 phishing sites** seeking personal information such as passwords and credit card details
- **832 advance-fee frauds** where a large sum of money is promised in return for a set-up payment[2]

And that's only in the UK. Bad actors aren't taking time off, so you, your IT teams and end users all need to be ready now for the increased security risks in this new age.

[1] "Remote Working: The New Normal?" Casey Rue, Forbes, May 20, 2020.

[2] "GCHQ calls on public to report coronavirus-related phishing emails," Alex Hern, The Guardian, April 20, 2020.

A two-part security challenge: Volume and security

Like so many other companies making the decision to shift to remote everything, your company's first challenge was how to ensure unimpeded performance for your remote workers who are trying to access their tools and data—or just find a reliable internet connection.

Following close on this first issue is the question of security. Suddenly it's the ultimate bring-your-own-device (BYOD) world. Every employee is now remote, and more focused on being productive than following your pesky security procedures. They'll access the data they need however they can; often bypassing VPNs to access cloud services or grabbing hotspots wherever they can—secured or not. This do-it-yourself attitude can lead to risky activities beyond your control, such as employees downloading software on their own.

With everyone using whatever devices are handy—personal phones, home computers, even kids' tablets (it has happened!)—the situation is especially perilous. One wrong click can instantly launch an attack that could jeopardise your entire business.

Given the limited capabilities of traditional perimeter firewall and VPN solutions to protect against these remote threats, companies need new security measures, new levels of expertise and new technologies to protect their assets. And the good news is you can build on current measures to get there.

Time is not on your side: Get a handle on your security picture

If you haven't had time to perform basic endpoint hygiene and connectivity performance checks on your computers and devices, better late than never. In addition to confirming all your laptops have the necessary endpoint protection configurations for all this new off-LAN activity, ensure your employees are following recommended security practices by asking these three important questions:

1. Have you reviewed and adjusted the security settings of your cloud tenant and your organisation's internal network?
2. Have you made sure the security settings and measures for remote users are appropriate for current and foreseeable levels of usage?
3. Are your team proficient in all of the latest security threats or do they need help?

Make remote workers the centre of attention

Remote workers are now the core of your productivity. The devices they work on can no longer exist at the edge of your security planning; they are dead centre and must be treated as such starting now. All that mixing and matching of personal devices with company equipment demands different practices and elevated controls. That means much more than the basic antivirus and antispyware protection, including multi-factor authentication (MFA) and onboard endpoint detection and response (EDR) capabilities.

Not only should your remote workers be aware of these new measures, but the tools and safeguards you use to attain and remain at a new level of endpoint and data security should meet those needs.

With the world rapidly—and permanently—changing, now is the time to enlist the help of a partner that has already worked out the best practices to face it. Without this critical help, you can't be sure each endpoint requesting access to internal resources meets security policy requirements. You need the right tools to track and enforce policy on all devices and with employees everywhere, while delivering easy user onboarding and offboarding.

We can help.

How the right security moves your business needle

Go beyond locking the gates. Lock in growth.

Your cyber security choices can have a dramatic effect on reducing your operational costs, improving employee productivity and satisfaction, boosting customer service, reducing risk and growing your business. CMI security services go beyond protecting your valuable data. By providing an outsourced, or co-sourced team for IT-as-a-service at any level, we offer you a revolution in your staffing model powered by our unique **Impact360** framework that moves your business forward.

Measurable, positive impact throughout your business

We developed **Impact360** as a revolutionary consulting framework built on Microsoft technologies. It enhances your business security and growth by ensuring over 200 performance standards, continually gathering actionable feedback from all across your business to inform the creation, delivery and optimisation of technology for measurable positive impact. Think of it as a constant feedback loop to support your staff in producing their best work—securely, happily, anywhere.

Enhanced security responses for the new remote work environment

The decentralisation of the workplace makes endpoint security more critical than ever. And the new tactics used by malicious actors require focus on different tools and solutions. If your organisation uses Windows 10 or later, **odds are you already have access to the world-class antivirus and antimalware solution already built into the operating system.** You also probably have the cloud licence to activate the centralised management and greater capabilities of Microsoft Defender.

Microsoft Defender for Endpoint gives you unmatched breach remediation and research capabilities. With a graphical representation, this tool enables security teams to map the precise point at which an attacker entered your network, how the attacker moved once inside and the activities they engaged in.

It is one thing to remediate a network breach but having the rich details of exactly how the breach occurred enables you to make sure any vulnerabilities in the network are found and corrected to prevent future breaches.

Here are three ways we can help you immediately to leverage your current Microsoft Defender technologies to face security challenges now and in the future:

Three ways to enhance security now

1. Phishing: Be the one that got away

Social engineering has always been a successful vector for malicious actors. But now with more employees working on their own, the bad guys have more targets of opportunity. With cloud providers hardening their security more than ever, phishing for credentials and spoofable material is becoming a path of least resistance. Once they have convinced a user to give up their sign-in information, hackers can accurately spoof the emails of internal users. The user receives an internal email, clicks on the link and that's it. The links lead to websites that look very real. For example, they might mimic the Microsoft Office 365 sign-in page. When a user enters credentials on this site to sign in, the bad actor then has access to your environment for further attacks.

Phishing is successful because even with the proper training, anyone can be fooled. So training must be regularly performed and reinforced through simulated activities—just like fire drills—to remind users to be sceptical of any email they receive.

If a single phishing attack gets through, it can cost your organisation hundreds of thousands of pounds, and a reputation damaged beyond repair. Just look at the news in the last several years. For training that's unmatched, Attack Simulator for Office 365 uses the Microsoft Intelligent Security Graph. It's constantly learning from global signals received from one of the largest telemetry systems on the planet. For example, Microsoft Office 365 scans 400 billion emails every month and finds a large number of malicious spear-phishing emails. The Attack Simulator carefully crafts simulated spear-phishing emails based on this real data, ensuring the most realistic attack experience for your user population. It then tracks and reports on user responses to the simulated email security events, providing invaluable data on how to better secure the organisation.

Three ways to enhance security now (continued)

2. Watch out for well-intentioned 'shadow IT'

As we've said, the new remote world of work is full of bright end users. They're bound to think they have better tools than those your IT department authorises. And they will use them. Sometimes a tool can go internally viral, becoming the app-of-choice before IT can stop it, or even become aware of its existence. Though your users see these as smart and cool new solutions, and see themselves as taking initiative to deploy them, they're dangerous to your data security and can obviously become the source of network breaches. We can help you through our managed security service to continuously monitor for these unsanctioned applications and the 'shadow IT' they engender.

3. Keep your defences strong

We can help. Your known tools can help protect you from unknown new threats—if you know how to use them. Our team of security experts will help ensure that your company's critical data protection is innovative enough to stay ahead of the threat environment with tactics that include:

- Security alert monitoring of Office 365 with Security Score
- Baiting and trapping of threats using honey pots
- Setup of antivirus active threat monitoring and mitigation
- App installation monitoring to prevent "shadow IT" behaviours with Device Guard
- User data classification setup
- Simulations of email phishing attacks raising awareness
- Simulated password spray and brute force password attacks to better secure credentials

CASE STUDY

Improving security while reducing costs

Company

Our client is a property investment firm specialising in large, complex, landmark developments in central London.

Challenge

The company felt they were falling behind their competition on the services they could provide to their clients—a very demanding audience of high-net-worth individuals. More immediately, they were exposed to significant security and compliance risks from outdated practices and poor staff awareness.

Solution

The client turned to CMI and our **Impact360** framework to provide a very direct alignment between their business objectives and IT strategy.

Working closely with the leadership team, CMI quickly made a plan to improve the baseline security posture, through improved security practices, hardened infrastructure and application security and higher staff awareness through security training. All this was part of a digital transformation programme for Microsoft Teams, SharePoint and the wider Microsoft 365 suite to improve collaboration, productivity and ultimately, customer service levels.

Results

The programme has resulted in measurable business, cost and security improvements including:

- A 13% drop in security-related service tickets, saving resources, money and risk
- A 21% improvement in staff happiness with their ability to perform their roles effectively

Find your security gaps—FREE

Contact CMI Now for a **FREE Impact360 Security Gap Analysis** to reveal your potential vulnerabilities and risks while indicating ways your business can benefit from improved security.

START NOW

cmi

Microsoft 365