



Redesigning Security in the Modern Workplace

When 20 offices becomes 20,000 workplaces





Unprecedented circumstances across the world have been a catalyst for accelerated remote working. Businesses have been forced to activate, at speed, continuity plans to support thousands of people working from home like never before.

In many cases, 20 offices became 20,000 workplaces almost overnight. This dramatic increase in endpoint locations, means that IT leaders and decision makers need to rethink cybersecurity strategies, reassess risks and adapt security infrastructures to enable new ways of working.

It is crucial, that while the evolving nature of the office and need for remote working must be considered, businesses must also look at ways to integrate these new ways of working into their wider digital transformation plans.

As businesses try to manage an evolving hybrid home/office working arrangement as the new norm, it is critical to enable employees to work in agile and mobile ways, outside the four walls of the office without compromising the integrity of document and data security.

“

45%

of IT leaders say their company isn't fully set up for remote work; they're bridging these gaps by strengthening security and providing enhanced support to home users”¹

With remote work bringing heightened challenges, teams must feel empowered by secure and resilient solutions, that are supported by the right knowledge, technology and infrastructure. As it stands, print infrastructure is viewed as one of the top security risks by businesses.²

Security and data breaches have serious implications to businesses, with potential repercussions too big to ignore. This ranges from the protection of confidential individual and network information, as well as the reputational, legal and financial losses that can be incurred as a result of a cyber attack.

With remote working here to stay, the role of IT leaders is clear:

1. Assess the new vulnerabilities and risks
2. Reduce exposure to data hacks, leakage and breaches
3. Provide employees with a consistent technology experience and remote security policy

The exposure to security threats and increased security vulnerabilities from a remote workforce stems from a rise in the number of connected devices or endpoints, with each of these endpoints under threat from a new generation of malware and phishing attacks.

Mobile technology and personal devices have quickly become a primary security focus of businesses to ensure their systems, networks and data remain secure outside of their controlled office environments.

In turn, businesses are rethinking which devices to purchase and deploy as well as expediting the adoption of technologies and cloud computing initiatives to support remote work.

Now, more than ever, IT decision makers must adapt and navigate the constantly evolving threat landscape inherent with the remote working terrain.

“

70%

of medium and enterprise businesses agree that a more distributed workforce raises security risks and processes”³

Key considerations for a remote security strategy:



Educate employees on best practices when working remotely. This includes actions like minimizing personal activity on work computers and avoiding public Wi-Fi networks.



Ensure you are equipping your workers with the correct devices and security settings and discourage use of personal systems for any business activity.



Ensure all endpoint devices are up-to-date with the latest firmware to ensure optimal security.



Shorten patch cycles or set up automatic firmware updates selected where feasible to ensure up-to-date security is in place.



Utilize cloud platforms and applications that are built with security in mind, enabling a more flexible, scalable and dynamic work style.

“

Legacy systems simply do not have the capabilities to keep up with the evolving security threats, and relying solely on human oversight would prove woefully inadequate. Capable automated systems that can monitor, detect, manage, and prevent cyber attacks in real time will be what drives cybersecurity going forward.”⁴

Attila Tomaschek

Cybersecurity Researcher at ProPrivacy



How HP can help

As a trusted partner for organizations like yours, HP can help enable a secure and adaptive workplace across devices, data and documents.⁵

Answer a few quick questions to [find out how your print security rates](#), and then get a complete summary of recommended actions to close any gaps.



[Learn more](#) about how HP MPS can help you redesign your security strategy. Speak to a member of the team today.



References

- ¹ Remote work changing landscape: IT Leader View, HP, May 2020
- ² Quocirca, [Global Print Security Study](#), February 2019
- ³ Remote work changing landscape: IT Leader View, HP, May 2020
- ⁴ <https://www.disruptordaily.com/future-of-cybersecurity/>
- ⁵ IDC, [IDC MarketScape Worldwide Security Solutions and Services Hardcopy 2019-2020 Vendor Assessment](#), Dec 2019

