The hybrid workplace: What does it mean for cybersecurity?

Issued by ESET

2 Aug 2021

As we adapt to a new normal, remote working seems like it's here to stay. The model that appears to be gaining most traction is a hybrid one, where most staff are allowed to spend some time working from home (WFH) but will also be required to come to the office for at least part of the week. It is intended as a 'best of both worlds' solution for staff and employers. But as we have seen over the past 12 months or more, mass remote working has also created the perfect conditions for threat actors to thrive.

With more time to operationalise the switch, combined with the experiences of the past year, IT security leaders and their teams will be better prepared than they were in early 2020. But many business leaders admit to still being vague on the details of hybrid working. Any new security strategy must focus on both human and technology, particularly cloud-based, risks. Carey van Vlaanderen, Eset Southern Africa CEO, says: “Every business must fully be responsible for protecting their information, being informed on technology is a priority- businesses should not only ensure that they understand hybrid working, but the challenges they may face with this model as well.”

What’s hybrid working and why now?

The move to hybrid working seems inevitable. Managers were surprised to find that productivity didn’t fall off a cliff as many had predicted and employees found they were able to save time and money due to less commuting. Technology stepped in to fill the void with online collaboration, company-issued laptops, and cloud infrastructure empowering and supporting a new way of working.

Now that there’s light at the end of a long Covid-shaped tunnel, with the government opening the vaccine rollout, things are unlikely to return to the way they were pre-pandemic. According to Microsoft, two-thirds (66%) of business leaders say they’re considering redesigning office space, while 73% of employees want to stay flexible with working options, and 67% want more in-person collaboration. A new hybrid model will be an important way to improve staff well-being, retention and

recruitment, drive productivity and re-energize the workforce – not to mention justify expensive inner-city office space.

ICT

A new business offering for a new business world

ESET 24 Feb 2021

The security challenges of the hybrid workplace

“New ways of working from home can also increase employees and companies' cyber risks,” continues Van Vlaanderen. ESET research from earlier this year found that 80% of global businesses are confident their home-working employees have the knowledge and technology needed to handle cyberthreats. However, in the same study, three-quarters (73%) admitted they are likely to be impacted by a cybersecurity incident, and half said they’d already been breached in the past. This kind of disconnect does not make for coherent cybersecurity planning.

There are in fact multiple challenges facing organisations – many of which were witnessed first-hand during 2020 and the first part of 2021.

These include:

The human element

Ask any cybersecurity professional and they’ll probably tell you that the weakest link in the corporate security chain is the employee. That’s why we saw phishing campaigns repurposed *en masse* during the early days of the pandemic to lure users desperate for the latest news about the crisis. In April 2020, Google claimed to be blocking over 240 million Covid-themed spam messages each day, and 18 million malware and phishing emails.

Home workers are more exposed because they may be distracted by housemates or family members, and therefore more likely to mistakenly click on malicious links. Contacting IT support or even getting a colleague to sanity-check a suspicious email is much harder when working remotely, while personal laptops and home networks may also offer fewer protections from malware.

Technology and cloud-specific challenges

The heavy adoption of new cloud services also drew the attention of threat actors last year. There are persistent concerns over vulnerabilities and user misconfiguration of SaaS offerings, as well as reports of stolen account passwords and anxiety over the commitment of some providers to security and privacy. It’s telling that 41% of organisations polled by the Cloud Industry Forum still believe the office is a safer environment than the cloud. Moreover, a hybrid workplace will arguably require even more shuttling of data between remote workers, cloud servers and office-bound employees. This complexity will require careful management.

ICT

Avoiding the consequences of data loss

Gareth Tudor 29 Aug 2013

How do I plan for a more secure hybrid workplace?

The good news is that, while securing the new hybrid workplace will be challenging, there are best practices that can guide Chief Information Security Officers (CISOs). The Zero Trust model is gaining in popularity to manage the complexity of on-premises and remote, cloud-based workers and systems.

Led by internal deployments at Google, Microsoft and other tech pioneers, it's based around the premise that the old notion of corporate perimeter security is now defunct. Today, devices and users within the corporate network are no longer to be blindly trusted. Instead, they must be dynamically and continuously authenticated, with access restricted according to 'least privilege' principles and network segmentation put in place to further limit potentially malicious activity. It will require multiple technologies to work effectively, from multi-factor authentication (MFA) and end-to-end encryption to network detection and response, micro-segmentation and more.

That may not be within the reach of every organisation today, especially those with fewer resources to throw at the problem. In the meantime, there are some useful best practices outlined here. Before even thinking about new security controls and technologies, organisations must rewrite their policies for the new hybrid workplace. This should include access rights for individual employees, remote connection processes, off-site data handling, and users' cybersecurity responsibilities, among many other elements.

Finally, while technical measures like prompt patching are obviously vital, so are human considerations. Regular training and awareness sessions, delivered via bite-sized lessons for all employees, are a crucial component to enhancing any organisation's cybersecurity posture. They may be your weakest link, but staff are also your first line of defence.

About ESET

For more than 30 years, ESET® has been developing industry-leading IT security software and services to protect businesses, critical infrastructure and consumers worldwide from increasingly sophisticated digital threats. From endpoint and mobile security to endpoint detection and response, as well as encryption and multifactor authentication, ESET's high-performing, easy-to-use solutions unobtrusively protect and monitor 24/7, updating defenses in real time to keep users safe and businesses running without interruption. Evolving threats require an evolving IT security company that enables the safe use of technology. This is backed by ESET's R&D centers worldwide, working in support of our shared future. For more information, visit www.eset.com or follow us on LinkedIn, Facebook and Twitter.

- **Eset launches solution to address SOHO security concerns** 15 Apr 2024
- **Don't gamble with your cybersecurity** 29 Feb 2024
- **Avoiding job scams, and finding a job you love** 9 Feb 2024
- **Sharenting and security concerns: Will you be posting that back-to-school photo?** 10 Jan 2024
- **Fighting the digital grinch: Cybersecurity tips for kids and parents for a safe festive season** 8 Dec 2023

ESET

ESET has been helping people protect their digital worlds for more than three decades. From a small, dynamic company we've grown into a global brand with over 110 million users in 202 countries.
Profile | News | Contact | Twitter | Facebook | RSS Feed