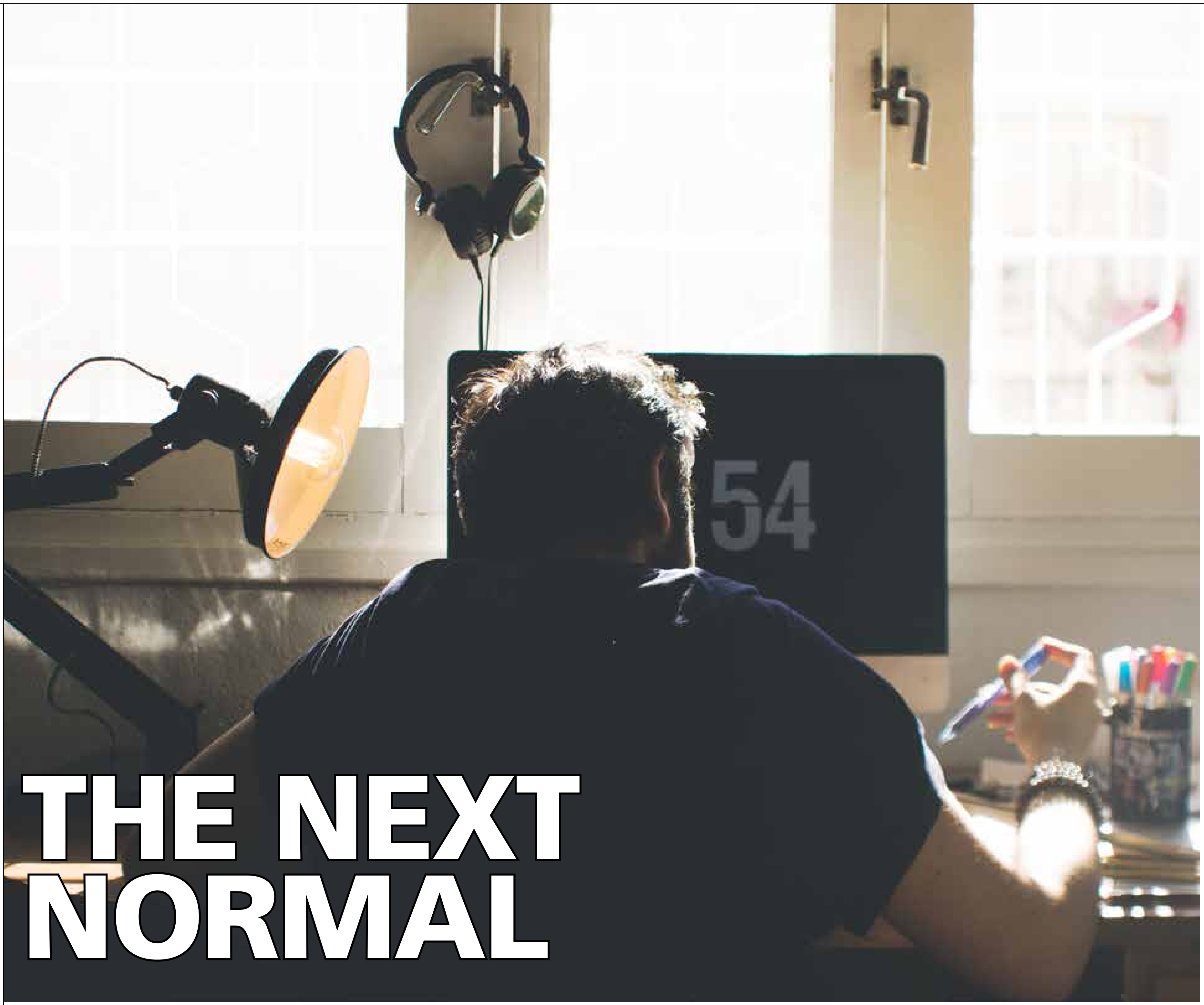

THE NEXT NORMAL

David Cummins *reveals the many threats that lay ahead in the new frontier for cybersecurity*

The COVID-19 pandemic affected every aspect of society, touching our personal and professional lives in ways few had seen before. As employers and employees were forced into their homes for months on end, communicating from behind closed doors and over screens, businesses were forced to adapt to an alternative way of working. The Office of National Statistics revealed in July 2020 that during the first national lockdown in April of that year 46.6 percent of the UK workforce completed at least some of their duties remotely. The study also showed that of those who did some work from home, 86 percent did so as a result of the global pandemic.

With such large numbers of the population conducting business operations from their own homes, the issue of protecting those systems and operations needed to become a priority for organisations. Unfortunately, the change in workflows, now existing on unsecured, sometimes personal devices and functioning in a multitude of locations, was also in the sights of cyber criminals. It has been reported that cyber-attacks against business increased by 20 percent in 2020 compared with 2019; the amount of attacks was said to reach 686,961, equating to one attack every 46 seconds.

The Forrester study explains that when working remotely over half of employees access customer data using their personal devices

A recent report conducted by Forrester Consulting on behalf of Tenable highlighted cyber risk as an increasing issue as attackers found new opportunities to enter company systems. It revealed that cyberattacks proliferate as organisations' attack surfaces continue to expand far beyond office walls: to home office networks, personal devices the cloud and third-party partners. According to the report, 92 percent of business and security executives surveyed stated that their organisation experienced a business-impacting cyber-attack or were compromised in the last 12 months. Of those surveyed, 67 percent also reported that these attacks specifically targeted remote workers and 74 percent believed that at least one attack resulted from vulnerabilities in systems put in place as a response to the COVID-19 pandemic.

So, not only did the world face a terrifying pandemic, the world of work experienced crippling cyber attacks borne out of the move to remote working. The Forrester study explains that, when working remotely, over half of employees access customer data using their personal devices, and 77 percent have six or more devices connecting to their home network. That's a lot of data floating around in the ether, and brick-and-mortar walls have no defence against bad actors and malware, which now have far more points of entry to attack company systems. Not only are there more cracks through which hackers can slip, but security leaders themselves are not equipped to be proactive against such threats. When it comes to employee home networks and connected devices, almost half of security leaders said that they lack visibility, and just 33 percent felt they have enough staff to monitor their organisations' attack surfaces adequately.

Even as most aspects of society attempt to return to normal, it is clear that remote working is here to stay – at least to an extent. Companies are still erring on the side of caution when it comes to COVID-19, with 70 percent of UK organisations now supporting remote employees. After more than 18 months since the pandemic began, many businesses still have employees working from home five days a week and most are preparing for the concept of permanent hybrid working in the future.

A home office may feel secure; a single computer in the safety of your own house, after all, doesn't seem like it would be a high priority for hackers. But employers must not forget that a myriad of people and devices are constantly connected to the very same home network that links remote employees to customer data, intellectual property and systems. Remote workers have an average of eight devices connecting to their home network and that isn't counting other household members who have their own equipment, be it personal or for work. How are employers to maintain secure systems when the devices that require monitoring are no longer restricted to workplace perimeters or even to their own employees?

It is paramount, with such diversified home networks, that employees remain vigilant themselves when it comes to security. However, only 34 percent of home workers strictly follow their organisations' security guidelines and measures; this includes verifying their identity using multi-factor authentication, accessing company systems and data via VPN only, not connecting via public wi-fi and avoiding the use of personal devices for work.

The problem continues to mutate as one considers third workspaces such as cafés, hotels and co-working spaces. Post-pandemic, remote working enables employees to be anywhere as they complete their duties; an accountant could be running operations from the coffee shop around the corner, while the marketing lead might be dialling into Zoom calls from their local library. As flexible and pleasant as this is, remote working brings with it important and sobering security threats which must be addressed.

CYBER-ATTACKS AGAINST BUSINESS INCREASED BY 20 PERCENT IN 2020 COMPARED WITH 2019

The advances in cloud computing helped to limit the damaging effect of the COVID-19 pandemic on many businesses, enabling them to move vital functions onto digital applications, tools and services. Without such technology, it is unlikely that organisations would have been able to reroute to remote workforce models and adapt their business operations in weeks. Key business areas that were the most likely to go digital due to the pandemic were accounting/finance and human resources. In addition, large groups of employees were permitted access to sensitive intellectual property and data outside the office's perceived safe perimeter. These changes enable organisations to pivot their business operations and improve employees' experiences, setting the stage for increased risk.

Although cloud computing facilitates online collaboration and easy access, such access can also become available to malicious actors intending to exploit new vulnerabilities. Over the course of the past year, 62 percent of businesses and security executives say that their organisations suffered business-impacting attacks involving cloud assets. Shifting operations onto cloud-based solutions and expanding software supply chains facilitated more points of entry for attackers. In fact, six out of 10 security and business leaders report increased risk related to expanding their software supply chain. A key example of this kind of attack, made possible for hackers due to vulnerabilities in business supply chains and gaps in product security processes, was the SolarWinds attack on government and other systems. Few organisations have adequate visibility into the third-party vendors and partners upon which they rely – a luxury no one can afford.

Looking ahead, organisations are shifting out of crisis mode and working out how they fit into this new world of work. Though cloud-based solutions will undoubtedly play a large part in rebuilding

▶

and improving business operations post-pandemic, adequate security in these highly dynamic and disparate environments will be paramount.

REMOTE WORKING BRINGS WITH IT IMPORTANT SECURITY THREATS, WHICH MUST BE ADDRESSED

To effectively combat the increased cyber threat brought about by changes the pandemic caused, organisations need to bolster security across all threat vectors. Cloud-based productivity as standard will only become more dominant as enterprises step up their investment in collaboration and connectivity tools, allowing for flexible and hybrid working; security solutions must match the pace at which this technology develops. It is clear that lessons were learned during the pandemic given business and security leaders reported that cybersecurity, data privacy and supply chain visibility will be a more central part of their business continuity and disaster response (BC/DR) plans as they develop the next phase of their workforce strategy. In fact, two thirds of executives plan to spend more on vulnerability management, an essential facet of any business strategy to manage cyber risk. Remembering the vulnerabilities in organisational exposure to heightened risks and threats to data security in this new world of work will be essential. Businesses need to prioritise increased investment in solutions that will help address vulnerabilities that exist in their infrastructure.

Tech solutions are not the only place where investment will be vital over the next 12-24 months. The demand for security staff is also sure to rise as remote working takes over and offices shrink permanently. In fact, a recent survey conducted by Fortune in collaboration with Deloitte revealed that 75 percent of CEOs expect their office spaces to shrink in the future due to remote work. Investment in talent is an underestimated but valuable advantage against cyber threats, and contrary to popular opinion it is not an exclusive or difficult sector in which to hire. The key requirement for a career in cybersecurity is aptitude, and the required specific skills or role parameters can be taught.

The future of effective cybersecurity is proactive rather than simply responsive. Security leaders and executives need to implement sustained, high quality investment in both security solutions and industry talent, to best prepare for increasing threats to business from malicious actors. It will not be enough to respond to attacks as they occur; rather, forward-thinking and intelligent business practice should grow to include cybersecurity as an integral element to all that it does.

The pandemic has irrevocably shifted our attitude towards the office and hybrid working seems an inevitable future for all businesses where remote working is possible. Businesses should see this new prospect not only as a threat to business operations, but also as an opportunity to reinvent their cybersecurity capabilities and build a stable, secure foundation for the future ●

David Cummins is VP of EMEA at Tenable

Only 34 percent of home workers strictly follow their organisations' security guidelines and measures