
Since January 2020 Elsevier has created a COVID-19 resource centre with free information in English and Mandarin on the novel coronavirus COVID-19. The COVID-19 resource centre is hosted on Elsevier Connect, the company's public news and information website.

# The future of security in a remote-work environment

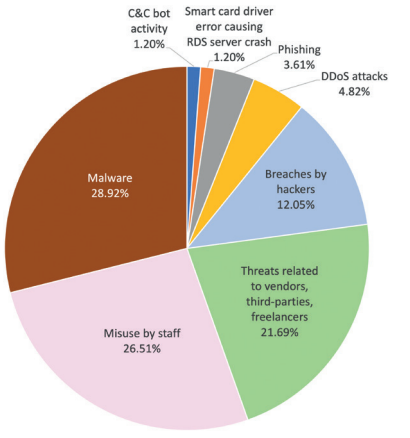
Jason Sabin

**Jason Sabin, DigiCert**

**Cyber security threats were a concern before the Covid-19 pandemic. But a year after businesses and employees vacated office complexes, the risks of falling victim to a cyber attack have only grown. In an article published by the Journal of Medical Internet Research, researchers found that the number of cyber attacks increased by 500% throughout the pandemic, and by 2021 are on track to cost world businesses $6tr annually.[1]**

Concerned about the toll that a hack could take on their own companies, global IT leaders have taken notice. Fudo Security conducted a survey showing that 42% of respondents said that Covid-19 had changed their cyber security priorities, and one in four said that their companies had already been victims of cyber attacks.[2] The surge in cybercrime has emphasised that businesses large and small need to take a proactive approach to protect their operations from the malware and ransomware attackers prowling the Internet.

***"To address both the challenges we face today and the ones that lie ahead, companies need to prioritise a robust digital infrastructure that is built for the future of work"***




What organisations see as the greatest remote access cyber security challenges. Source: Fudo Security

The new model of hybrid and remote work that companies worldwide are set to adopt will bring with it an array of challenges comparable to those of the earliest days of the pandemic. To address both the challenges we face today and the ones that lie ahead, companies need to prioritise a robust digital infrastructure that is built for the future of work.

## The threats

To cope with cyber security threats, companies must first recognise them. And perhaps the most notable threats that have arisen during the Covid-19 pandemic have been related to remote work.

During the ongoing pandemic, Pew Research recorded a 51% increase in the number of people working from home, a total of 71% of all participants surveyed. In the same study, 54% of people said they would prefer to work from home going forward.[3] Although this was not indicative of whether or not their companies would let them go remote or to what degree, it was indicative of the remote-work trend. Several security risks immediately are brought to the forefront as issues that companies should consider.

**Creating a security-focused culture**: Human error is the biggest threat to information security that companies face, and it can come in many forms. An employee who connects to public wifi without using a VPN; someone's child who uses their parent's computer and visits unauthenticated sites; an employee who gets a phishing email after a long day and clicks on the link without thinking twice – all are gateways to a data breach.

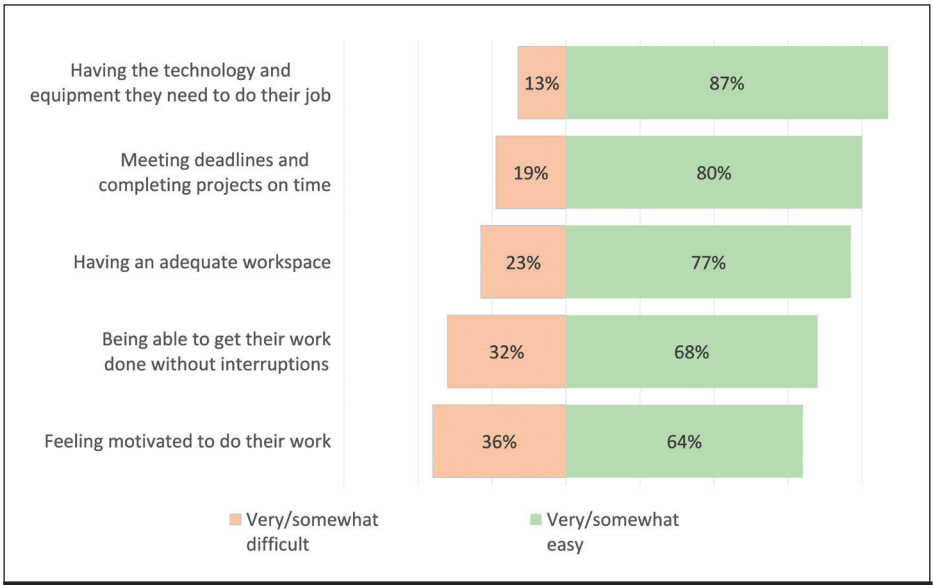
While no companies are 100% perfect, 100% of the time, one of the most proactive steps to take is to purposefully engage the entire workforce on where risks are the highest, what their common traits are, and the resources that they have available to them to protect themselves. Making sure that people understand the ramifications of a data breach is also important and why due diligence is the best weapon against attacks. Seminars and classes can also be helpful and can also be framed as helping employees protect their personal data.

**Device and account security**: It is commonplace for companies to issue laptops or tablets for work use, but often that technology does not cut it for employees when they work remotely. Many people access email on their phones, review documents on tablets, or use a more powerful desktop to get things done, even if it is company policy not to. This enhances the risk of password theft, ransomware or malware placement.

To combat the risks of remote device insecurity, companies should implement accessible security measures such as VPN and two- or multi-factor authentication to protect employee data, and institute an enterprise-wide mobile device management policy. They should also emphasise secure password protection and management, such as what makes a good password and encourage the use of secure enterprise password management tools.

**Safely using the cloud**: The cloud is remote-friendly by nature, and many companies finally made the shift after being forced to collaborate away from the workplace. While it may have been a heavy lift for companies used to keeping data onsite, what it lacks in ease it makes up for in security.

Particularly for small and mid-sized businesses that were less inclined to




How newly remote workers found various aspects of working from home. Source: Pew Research.

invest in enterprise-level cloud computing before the pandemic, doing so offers a similar level of security to onsite data storage and is significantly more practical. Cloud operations offer end-to-end encryption, privacy controls and maintenance controls that keep systems up to date. Vulnerability testing is another common tool that cloud vendors use to evaluate risk and secure operations.

## Future-proofing

It is likely that many of the pandemic-era workplace policies will stay in place. The most apparent result of that will be employees continuing to work from home, in some cases permanently, but in most circumstances on a hybrid basis. The new working arrangements bring to the forefront the issues of combating cyberthreats for employees who are no longer in the same building – a challenging task, but not an impossible one.

The most significant challenge remains the same – working in an online environment that has not been adapted to enterprise-level security. The networks that people work on at home are the same ones that their kids watch Netflix on and to which their smart doorbells are connected. Wifi is rarely secured, and firewalls are mostly unheard of for home networks. To adapt to those challenges on an enterprise level and for the long term, it is critical for companies to scale VPN access to all secured devices and create a zero-trust zone that requests credentials for every login. Two-factor authentication is even more secure. Such measures are crucial steps to making sure that even if bad actors gain network access, they face barriers to breaching actual information systems.

Companies will also face the tragedies of human error during the transition to new work models. Like the vulnerable positions they were in during the initial transition in spring 2020, as employees adapt to new circumstances, cyber security can fall by the wayside. The result could be clicking attachments to messages disguised as return-to-work guidance, vaccination protocols, or other appropriately timed subjects, all of which could serve as an entryway to the broader network.

Malware and ransomware are also not always used immediately by bad actors. A common practice, and one that is particularly threatening to companies with employees who are about to re-plug into the corporate network for the first time, is malware that has been installed but is dormant. While most endpoint security systems offer protection against most threats, they do not offer the certainty of a firewall, so companies would be wise to mitigate risk by implementing zero-trust quarantine policies, in which IT departments would scan each and every returning device before it returned to the network. The vetting process would cleanse the entire system of threats, literally before they arrive.

## Next-generation threats

The remote transition that took place in early 2020 was chaotic, to say the least. As businesses eye the short- and long-term futures of their workplaces this time around, they have the luxury of being afforded more time and resources to make a more efficient and well-thought-out transition. The workforce plans that they will implement are also likely to be the ones that they will live with for decades to come, so making security a priority when building them will ensure a strong foundation for new threats that arise.

**Enhanced phishing techniques**: Phishing attacks have spiked by 350% during the pandemic, and they are only going to become more frequent and sophisticated as time goes on.[4] Cyber criminals took notable advantage of the Covid-19 crisis from the beginning, using it as an opportunity to ensnare people in links to phony CDC guidelines or health advisories. Attackers will certainly continue to use the guises of vaccination instructions or requests to share personal information in return for health data. In more extreme scenarios, criminals could even request addresses and use them to arrive at employees' houses and hack into home networks.

***"A common practice, and one that is particularly threatening to companies with employees who are about to re-plug into the corporate network for the first time, is malware that has been installed but is dormant"***

**Home network attacks**: If workers are bound to their home networks, hackers will certainly try to follow. Rather than using energy and resources to breach a corporate network onsite, a cheaper and likely easier option for cyber criminals is to breach under-protected home networks and through that window enter corporate networks.

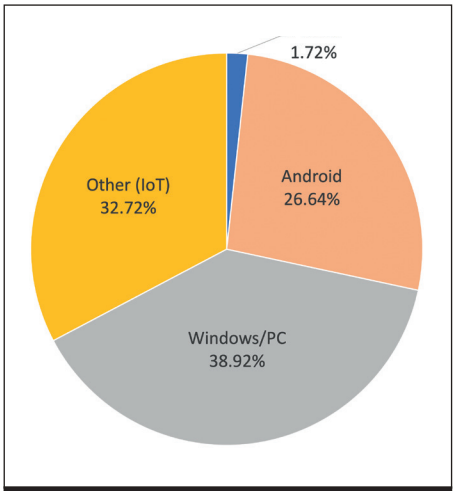
Security measures that companies can take to combat this future threat are

uncertain but include better employee education and offering resources to protect homes. However, the strongest approach is to continue to provide cloud-based patch and endpoint management.

**Supply chain attacks**: One of the more sophisticated attacks that companies are seeing on the horizon exploits the vulnerabilities that come from known, third-party software – tools routinely trusted by employees and tech experts alike – that are planted into coding or servers and migrate into devices when they undergo routine updates. By changing source code, such attacks often go undetected because third parties are unaware that the coding has been infected. Endpoint machines themselves are also none the wiser because the malware runs under the same permissions as the unadulterated app would.

***"Companies can mitigate many of the risks related to them by employing strong code integrity protocols and only allowing verified applications to run on enterprise systems"***

Supply chain attacks are particularly harmful because of their ability to infect many devices quickly. But companies can mitigate many of the risks related to them by employing strong code integrity protocols and only allowing verified applications to run on enterprise systems. Strong endpoint management systems are another strong tool to mitigate risks.




**A breakdown of infected devices in the enterprise. Source: Nokia**

**Distributed denial of service (DDoS)**: This is a tactic used to overwhelm whole networks rather than individual employees. As hackers become more fluent in gaining access to devices, they are more frequently using those devices as tools to disrupt operations at unsuspecting companies. Directing the attention of an entire botnet to a single corporate website is an effective way to quickly disable a website for either ransom or activism.

To combat this new wave of cyber attacks, best practice dictates that companies retain third-party firms with advanced expertise in DDoS defence, and their capabilities for blackhole routing, rate limiting, network diffusions and strong firewalls will be far beyond any enterprise-level hardware on the market today.

**Attacks on the Internet of Things (IoT)**: To the dismay of companies and employees alike, hackers are becoming proficient in invading devices beyond computers. As speakers, watches, home security systems and even refrigerators become Internet-enabled, they also become targets for malware.

A report from Nokia found that IoT devices made up nearly 33% of infections in 2020, a number that is sure to rise as the Internet becomes fluent in more devices.[5] The threat is serious for devices on home networks, but also will extend to AI used in the workplace and on the manufacturing floor, threatening the stoppage of essential operations if hacked. User education is critical to mitigating the threat of IoT attacks, and alongside two-step authentication, segmentation from the network, and software updates, can go a long way towards digital safety.

## The new normal

Whether the new normal is completely remote, hybrid, or mostly in-person, addressing the security threats that have been emphasised by Covid-19 will be paramount to any return-to-work strategy.

By strategising early and adopting plans that take into consideration current and future threats, not only will companies be able to avoid the collective chaos that ensued at the beginning of the pandemic, they will also be able to build a strong foundation for threats on the horizon – because if there is one thing we know for sure, it is that they are out there.

## About the author

*Jason Sabin joined DigiCert in 2012 and before being promoted to chief technology officer in 2020, he held roles including VP of research and development, chief security officer and chief information officer. As CIO, he spearheaded the move to SaaS and cloud services over on-prem instances. Sabin has more than 20 years of engineering and R&D experience working in the identity and security industry, with roles prior to DigiCert at NetIQ, Novell and Volera. He is a regular speaker at security, IoT and technology conferences. He has twice been named a Utah Genius for top inventor, with more than 50 patents issued.*

## References

1. Williams, Christina; Chatuverdi, Rahul; Chakravarthy, Krishnan. 'Cyber security Risks in a Pandemic'. Journal of Medical Internet Research, 17 Sep 2020, vol.22, no.9. Accessed Oct 2021. www.jmir.org/2020/9/e23692/.
2. '42% of security leaders said the pandemic has changed their cyber security priorities'. Help Net Security, 15 Dec 2020. Accessed Oct 2021. www.helpnetsecurity.com/2020/12/15/pandemic-cyber security-priorities/.
3. Parker, Kim; Menasce Horowitz, Juliana; Minkin, Rachel. 'How the Coronavirus Outbreak Has – and Hasn't – Changed the Way Americans Work'. Pew Research Center, 9 Dec 2020. Accessed Oct 2021. www.pewresearch.org/social-trends/2020/12/09/how-the-coronavirus-outbreak-has-and-hasnt-changed-the-way-americans-work.
4. 'UN reports sharp increase in cybercrime during pandemic'. Associated Press, 7 Aug 2020. Accessed Oct 2021. https://apnews.com/article/virus-outbreak-counterterrorism-health-crime-phishing-824b3e8cd5002fe238fb9cbd99115bca.
5. 'Threat Intelligence Report 2020'. Nokia, 2020. Accessed Oct 2021. https://onestore.nokia.com/asset/210088.