MORPHISEC
Moving Target Defense

MORPHISEC'S 2020

WFH EMPLOYEE CYBERSECURITY

THREAT INDEX

OVERVIEW

As companies across the globe continue to participate in the largest work-from-home experiment in history, it's no secret that many serious questions have arisen about the cybersecurity of remote endpoints and network infrastructures.

Subjected to spotty home-based WiFi networks and non-hardened devices operating outside corporate network security controls, the challenges today's workforce face are enormous and undoubtedly compounded by the additional pressures they're under to remain productive from home. It's certainly a stressful time for all, and in particular for security professionals who feel the burden of protecting remote workforces that seemingly appeared overnight.

In fact, the repercussions have been making regular headlines since much of the U.S. was forced into quarantine. With many corporations turning to collaboration apps for video conferencing and instant messaging to stay connected, their workforces rely on vulnerable tools that are in the crosshairs of malicious parties that understand their weakness and inefficiency with patching.

These vulnerabilities have forced many organizations such as Google, SpaceX, and even NASA to actually ban employee use of such applications in fear of more sophisticated breaches. Morphisec Labs researchers discovered one such flaw in the Zoom application that enables threat actors to record Zoom sessions and capture text chats without the participants' knowledge.

However, by most productivity accounts, this rapid migration to work-from-home environments in response to COVID-19 has been a success and executives now see remote work as a viable option at scale. So as leadership teams plan for more agile and remote workforces post-pandemic, they will need to look at new ways to evolve their IT infrastructure and security stacks to better protect their workers from cyber threats outside the walls of their offices.

KEY FINDINGS

As Morphisec continues to assist now distributed organizations with improving their cyber defenses and protecting their remote employees, it commissioned its first-ever **Work-from-Home Employee Cybersecurity Index** to examine how organizations and employees were coping with the changes. A survey was administered in April 2020 to 837 U.S. office workers that self-reported as recently transitioning to working remotely during the response to the COVID-19 pandemic.

Here's what we found:

WFH IS AN ENTIRELY **NEW EXPERIENCE**

Work from home is an entirely new experience for a huge percentage of the American workforce with almost half (49 percent) of respondents stating they had never worked remotely before.

56 PERCENT ARE USING THEIR OWN **PERSONAL COMPUTER**

56 percent of employees are using their own personal computers as their work device during the crisis and 23 percent are unsure of what security protocols are on the device they are using the most during this work-from-home period.

SPOTTY WIFI **DURING QUARANTINE**

More than 1-in-4 work-from-home employees have frequent or more issues with spotty WiFi during quarantine. This could be impacting the usefulness of antivirus software, which needs connectivity to stop threats.

EMPLOYEES ARE CAUTIOUS WITH OFFICE 365

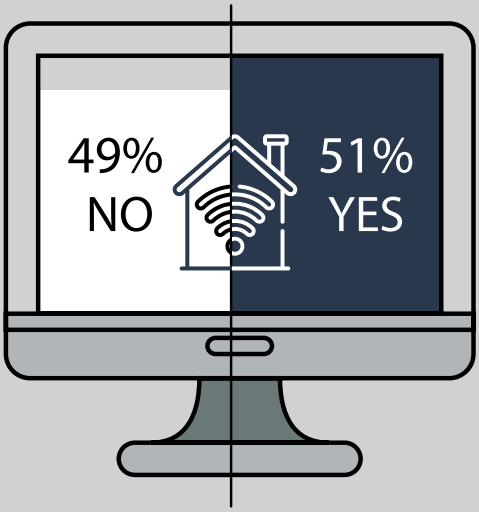
More work from home employees (39 percent) said they were "most cautious" in using productivity suites such as Office 365 versus business chat applications (10 percent) when it came to cybersecurity hygiene, despite both categories being considered the most essential of all the apps they currently use.

THE NEW FRONTIER OF REMOTE WORK

While it's true that COVID-19 has indisputably magnified concerns across the board, the cybersecurity risks of working from home aren't all that new. Employees were already starting to work from home more often; in fact, according to FlexJobs, the number of remote workers grew 44 percent between 2014 and 2019, and 159 percent between 2005 and 2017. Similarly, according to Owl Labs, 56 percent of global companies already allowed their employees to work from home.

These remote employees already created additional risks for cybersecurity and IT professionals in terms of ensuring they could securely access the information they needed. This is a well-trod concern among security professionals and C-suite leadership. That said, although the concerns are not new, the scale on which they need to be addressed is. Of the employees who have transitioned to working from home during the response to the COVID-19 pandemic, a staggering **49 percent had never worked remotely before.**

Q Prior to the COVID-19 pandemic did you ever work remotely?



Working from Home Is a Completely New Experience for Nearly Half of Office Workers

In addition, of the **51 percent** who had worked remotely before stay-at-home advisories and orders came into effect, most (45 percent) only did so once per week. Furthermore, just under a quarter (24 percent) said they worked from home twice-per-week, while 31 percent worked from home more than twice a week pre-pandemic.

Add in the stress for many remote workers to simultaneously be productive and educate their out-of-school children, and it becomes clear that there are far more challenges inherent in the current work-from-home environment than normal. The sudden influx of remote workers also puts additional strain on IT professionals, who must now ensure that all these new remote employees can safely and securely access the tools they need.

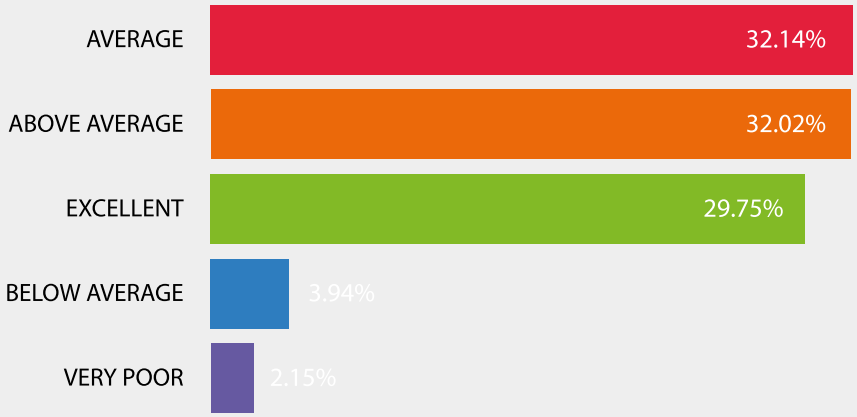
HOW IT IS COPING

The sudden surge in work-from-home employees has placed enormous strain on IT departments at office-based businesses. In general, IT and security professionals have either the ability to manually add additional security measures to a remote employee's company-provided machine, or the time needed to spin up alternative ways (such as a virtual desktop infrastructure or virtual private network) for employees to access the systems they need in a secure fashion.

62% of WFH Employees Rate IT's Response to COVID-19 Above Average or Better

The COVID-19 pandemic accelerated that timeline from weeks to days, which meant that IT had to quickly create the architecture they needed to shift oftentimes the entire company to working from home. With that said, respondents showed appreciation for their IT teams' response to COVID-19. Suddenly tasked with protecting the vast scale of remote workers who exponentially increase the attack surface, security professionals have experienced enormous strains on their resources and bandwidth.

Q How would you rate your company and IT department's response to putting the technology infrastructure and security measures in place so your workforce can now safely and productively work-from-home?



As a result, **62 percent of employees** rated their company and IT department's response in putting the appropriate technology infrastructures and security measures in place to ensure safe and productive working from home as above average or better. This is heartening to see as people continue to work from home, putting additional strain on the IT team to manage all the infrastructure needed to maintain security and accessibility from multiple remote locations.

HOW MUCH IS IT'S GUIDANCE FOLLOWED?

Naturally, the challenges facing these teams have been herculean at times. **Seventy-five (75) percent of workers said** they either usually or almost always follow the advisory of their IT department or security staff when it comes to cybersecurity protocols. The most common tip they received was to be wary of suspicious emails, attachments or pop-ups (56 percent). With Google reporting more than 18 million daily malware and phishing emails related to COVID-19 in just one week in April, it's hardly a surprise that this is IT teams' biggest worry for their remote colleagues. While phishing has left a long wake of disruption behind it in recent years, malware authors are leveraging the fear around COVID-19 to further their goals and deliver their payloads.

Meanwhile, the second most common tip respondents received from their IT teams was to ensure antivirus software was connected and active (48 percent). This was followed by updating software and patches frequently (46 percent). Research actually finds that 60 percent of data breaches are caused by exploiting a software vulnerability that was known but which the victim had not yet patched.

Finally, and perhaps most concerning given that employees spoke highly of their IT team's response to COVID-19, is that 20 percent of workers said their IT team had not provided any tips as they shifted to working at home. This is problematic for long-term security posture, especially because of the vulnerable nature of home WiFi networks in addition to the lower network protections that result from working remotely.

Be wary of suspicious emails, attachments or pop-ups	**472**	**56.39%**
Make sure antivirus software is connected/active	**405**	**48.39%**
Update software and patches frequently	**382**	**45.64%**
Create a backup of your data frequently	**256**	**30.59%**
Disconnect your device from the internet immediately if you believe you have been breached	**174**	**20.79%**
They didn't give any tips	**169**	**20.19%**

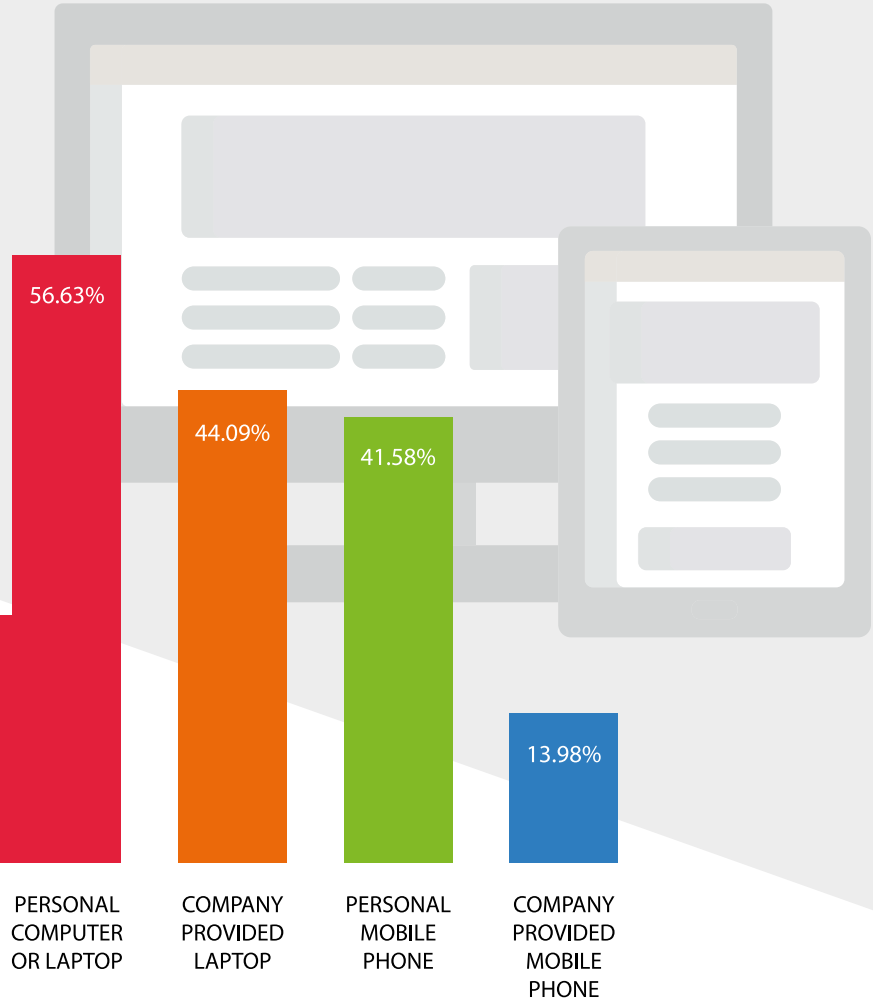
CHALLENGES FOR WFH SECURITY

Without security best practices in hand for some employees, it was concerning to find that **56 percent of workers use their personal computer or laptop for work purposes**. In addition, a further 42 percent admitted to using a personal mobile device for work-related tasks.

These non-hardened endpoints open up yet another gateway for bad actors to infiltrate network infrastructures and steal sensitive corporate information. The damage that can be inflicted by working on unsecured personal devices is substantial; research from Morphisec and Ponemon Institute found the average cost of a successful endpoint attack was $8.9 million in 2019, a stark increase of almost $3 million from the previous year.

Q What devices are you using for working remotely during this period?

56% Use Their Personal Laptop or Computer for Working Remotely

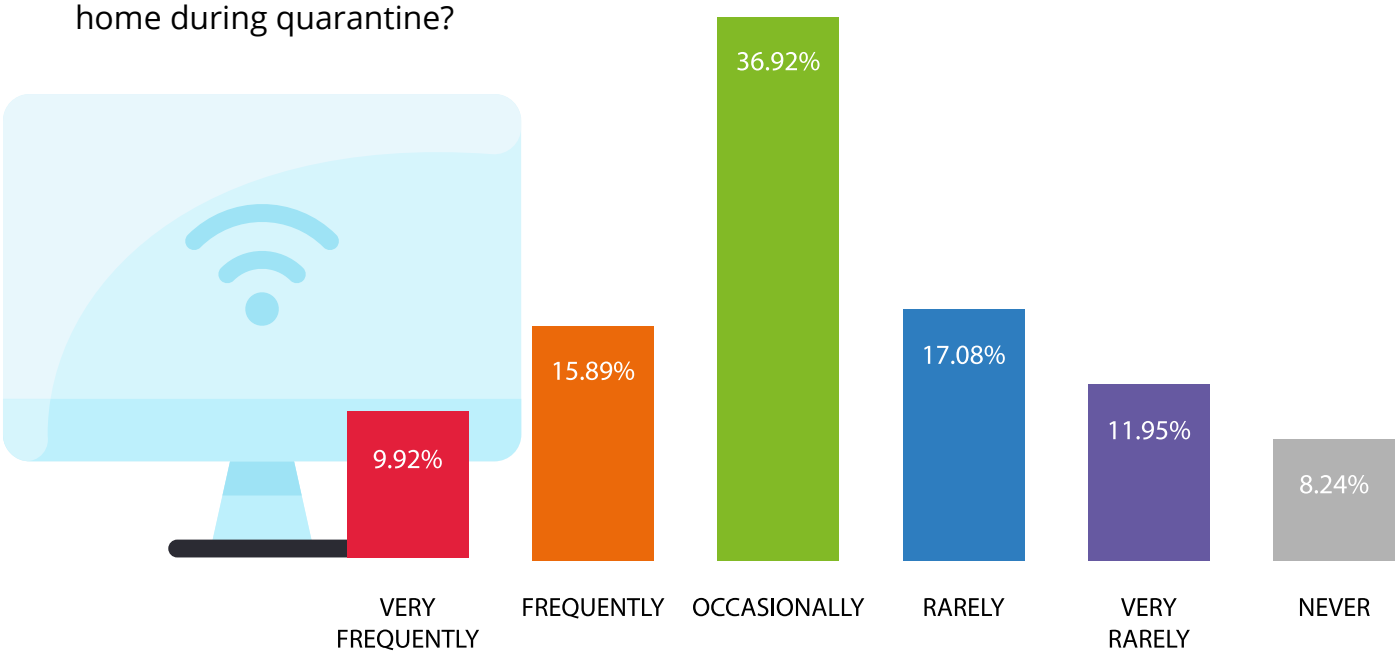


With the rise in people working remotely as well as the lure of Bring Your Own Device (BYOD) taking off pre-pandemic, the number of endpoints has exploded and created additional risks of cyber attack through additional points of vulnerability. COVID-19 is sure to amplify these weaknesses.

In fact, nearly 1-in-4 employees (23 percent) noted they didn't even know what security protocols or software they have in place on the devices they were using most for work since moving to work-from-home!

26% of WFH Employees Have Frequent Issues with Spotty WiFi During Quarantine

Q Have you had issues with spotty WiFi or internet speed while working from home during quarantine?



Most modern organizations, whether in the private or public sector, have extensive network monitoring and security tools in place. These include firewalls, network analysis and forensics, and email spam filters designed to catch malicious code and phishing attempts before they even access employee computers. But when an employee works remotely, all that protection goes away.

In fact, in a study on mobile workforce security, 81 percent of organizations reported they had seen WiFi-related security incidents in the last year, with 62 percent of these occurring in cafés and coffee shops.

With **26 percent of work from home employees reporting having frequent or very frequent issues with their WiFi connections**, they may not be getting the protection they need, even with antivirus software installed on their computers. Antivirus and detection tools need a constant network connection to be even slightly effective at blocking attacks and, in spotty WiFi scenarios, organizations and their employees are left exposed to compromised information, stolen credentials, and even malware.

With data breaches inflicting severe long-term damage on organizations, companies must utilize advanced threat protection alongside traditional antivirus in their security stacks, given its spotty efficacy in work from home scenarios.

It's no surprise that we've seen a massive surge in the popularity of collaboration tools that allow businesses and consumers to stay connected with the outside world. Apps like Zoom, Slack, Microsoft Teams, and WebEx have seen their user numbers skyrocket since companies started to enforce work from home decrees to flatten the curve. Zoom added more active users (2.2M) in January and February alone than it did in the entirety of 2019.

Business Chat Apps are Among the Most Essential Tools, Yet WFH Employees Are Not Cautious Using Them

Work-from-home employees in our survey were most likely to still rank productivity suites (39 percent) such as Office365 or GSuite as their most essential work application during the crisis. However, this was closely followed by business chat tools (17 percent) and video conferencing tools (16 percent). Both beat out word processing tools (13 percent) and email (12 percent) in terms of essential applications during their remote working.

The most essential work applications, tools or documents you are using while working-from-home:

Productivity Suites: Office 365, GSuite, etc.	**355**	**42.41%**
Business chat tools: Slack, Microsoft Teams, etc.	**140**	**16.73%**
Video Conferencing tools: Zoom, WebEx, etc.	**131**	**15.65%**
Email service: Outlook, Gmail, etc.	**107**	**12.78%**
Word processing tools: Microsoft Word, PDF, Google Docs, etc.	**104**	**12.43%**

Work applications, tools or documents you are most cautious in opening, sharing or using due to perceived cybersecurity risks:

Productivity Suites: Office 365, GSuite, etc.	**328**	**39.19%**
Video Conferencing tools: Zoom, WebEx, etc.	**174**	**20.79%**
Word processing tools: Microsoft Word, PDF, Google Docs, etc.	**128**	**15.29%**
Email service: Outlook, Gmail, etc.	**124**	**14.81%**
Business chat tools: Slack, Microsoft Teams, etc.	**83**	**9.92%**

However, this rapid ascension has also spotlighted severe security vulnerabilities. With that said, it turns out that work-from-home employees are not as cautious when relying on tools like Slack or Microsoft Teams. Just 10 percent said they are the most careful when using business chat apps compared to the 40 percent that said they were most cautious when using productivity suites. Meanwhile, it seems some of the recent security concern headlines with Zoom may be causing some workers to be more cautious when opening, sharing or using video conferencing tools (21 percent), despite relying on these tools slightly less than business chat apps.

This is even after a critical vulnerability was found in Slack in March that revealed significant gaps in its security that could allow automated account takeovers (ATOs) and lead to data breaches. In addition to exploiting security bugs, bad actors have other attack vectors when it comes to collaboration tools. For instance, apps like Slack and Microsoft Teams have messaging components that can be used for phishing attacks and to deliver malware payloads through links and attachments, just like in email, leaving businesses who are suddenly dependent on these tools for communication and connectivity particularly vulnerable.

Opportunistic by nature, hackers look for the easiest ways to attack the largest number of users and reap the biggest gains. And unfortunately, these applications check all those boxes right now, making them an appealing target for every cybercriminal in the world. Adversaries are mostly financially motivated and, except in rare cases, only focus on building exploits for the most widely used tools so they can get the best ROI for their efforts. And with spending on collaboration applications predicted to exceed $48 billion by 2024, it's no wonder that threat actors see dollar signs.

In addition, tools like these create higher risks for browser-based attacks and social engineering attacks. So despite their importance, the reality is that they're often unequipped for prime time. They simply lack robust security posturing which makes them especially vulnerable to zero-day attacks and evasive malware.

CONCLUSION

The trend toward remote work was already in progress when COVID-19 struck, accelerating the transition far faster than anyone anticipated. As a result, IT and security teams had to scramble to ensure everyone could access the tools they needed to do their jobs without coming into the office. Thus far, despite the increased risk of browser-based attacks and social engineering, companies have risen to the challenge of a work-from-home world. The task now is to ensure that remote workers remain secure as they do their day-to-day work and continue to work remotely now and in the future.

ABOUT MORPHISEC

Morphisec delivers an entirely new level of innovation to customers with its patented Moving Target Defense technology to place defenders in a prevent-first posture against the most advanced threats to the enterprise, including APTs, zero-days, ransomware, evasive fileless attacks and web-borne exploits. Morphisec provides a crucial, small footprint memory-defense layer that easily deploys into a company's existing security infrastructure to form a simple, highly effective, cost-efficient prevention stack that is truly disruptive to today's wexisting cybersecurity model.