COVID-19’s Impact on Organizational Cybersecurity Posture

By Douglas Shuman https://www.linkedin.com/in/douglas-shuman-06221b122/

Part one of this two-part article looks at some of the rapid changes that happened in the work place due to COVID-19 and their implications to cybersecurity.

Abstract
Organizational cybersecurity landscapes changed as a result of employees working from home during the COVID-19 pandemic. Abruptly sending employees to work from home resulted in many quickly implemented changes. This research is a review of the cybersecurity landscape of the transformed workforce. This includes the scope of pandemic telework, how threats changed, and the cyber-attacks observed. Organizations need to continually evaluate how they secure their environment to allow for remote work and ensure best practices are in place.

Introduction
When the significance of COVID-19 (“the coronavirus”) became clear in early 2020, many organizations’ cybersecurity landscapes changed as a result of sending employees home to work remotely. Government mandates were largely the source of sending employees home, with the purpose to stop the spread of a deadly virus which we knew little about. This introduced two new threats; “a high-profile event and a rapid change in computing habits.” [1] While working from home is not a new concept, starting in March and April of 2020, most U.S. organizations (e.g., businesses, government agencies) needed to continue operations with most or all employees now working from home. In the United States especially, organizations had little time to prepare for a crisis response that suddenly sent employees to work remotely.

To those who were uninvolved in making changes, the situation may seem like Information Technology (IT) departments simply made a few networking changes to implement remote work solutions or expand capacity. However, this assumption ignores the variety of decisions with serious cybersecurity implications that organizations faced because of increased remote work. This is apparent from a survey by the Information Systems Security Association (ISSA), which was sent to people working in cybersecurity and IT positions. Twenty-seven percent of respondents willingly indicated their organizations were underprepared to secure the devices and applications employees would use at home. [2]

At the time of writing, organizations have mostly moved on from the changes required to enable high-volume remote work to supporting remote work over the long term. Regardless, decisions with cyber-implications made during the beginning of 2020 are likely still putting organizations at risk. This begs the question: in light of COVID-19, how have organizations’ cybersecurity postures changed due to the influx of people working from home? There are many issues worth investigating because of the pandemic, but the focus of this research is on the impact of COVID-19 on organizations’ cybersecurity postures and how they have changed.

Literature Review
Significance and Scope of COVID-19 Work from Home
Not every company could allow employees to work from home when COVID-19 began affecting everyone. The U.S. Bureau of Labor Statistics finds that working from home is generally feasible in “management, professional, and administrative support jobs, but not in most service, construction, transportation, and production jobs.” [3] This study found that before the pandemic, about 45% of the U.S. employment population were in positions where telework (i.e. working from home) was feasible. [3] Of that surveyed population, the work from home “takeup rate” (spending a significant amount of time doing remote work) was about 22% or 25% depending on the survey. [3] To summarize, less than half the workforce had the capability to work from home, and about a quarter of those people took advantage of work from home.
Once the pandemic required organizations to enable work-from-home, employment drastically changed. Stanford research found that regardless of current occupation or employment status, in June 2020, 43% of the U.S. labor force was working from home. [4] A Gallup poll found that remote work leveled off around mid-April with a total of 63% of employed adults having worked from home at some point. [5] PricewaterhouseCoopers (PwC) performed a survey of office workers from May to early June and found every employee was working from home. [6] Of those PwC surveyed, 70% of workers were required to work from home due to shelter-in-place mandates (and they did not work from home before), while the other 30% were able to easily switch to full work from home given existing flexible arrangements with employers. [6]

The above statistics show that the organizations which allowed working from home before COVID-19 were accustomed to only a small amount of their workforce utilizing remote work. As a result, most organizations were unprepared for the massive amount of remote work that suddenly needed to be enabled. This encouraged hasty decisions with cybersecurity implications.

**Need for Agility**

IT departments need to respond quickly and flexibly given customer and business requirements. A pandemic is an extreme example of changing requirements warranting flexibility and timely responses. This is the purpose of the agile development process. Working from home during the pandemic has further reinforced the need for agility, especially regarding cybersecurity. [7] Even in 2021 Gartner is saying, “the pandemic has highlighted the challenges resulting from rigorous, inflexible security programs,” which shows the need for agile cybersecurity programs. [8]

Non-security IT teams often do not consider cybersecurity until after deployment, which is sometimes called “bolting on” security. This is the opposite of “baked in” security, which considers cybersecurity implications throughout changes and development, ideally in an agile manner. Lovejoy et al. found that just 36% of organizations say cybersecurity is built into their planning. [9] There are some significant concerns with considering security after planning, especially after deployments. Considering security after deployments can make implementation more difficult, and organizations are open to attack during the period where systems are vulnerable. We can expect cybersecurity was ignored regarding many changes due to COVID-19, because it is often initially overlooked in general.

**Enabling Pandemic Telework**

Organizations had to achieve many things to enable pandemic telework. At its simplest, working from home consists of an employee with an internet connection, a computer, and means to connect to their organization’s resources (e.g. by virtual private network), without physically being in a traditional workplace. The focus here will be the concerns of new working locations, types of devices connecting to the organization network, and types of remote access.

**New Location Concerns**

Working outside of the regular workplace (e.g. office) introduces different threats. Many organizations that suddenly needed to enable telework did not have time to address newly introduced threats. A concerning pandemic statistic shows that 45% of employees had no training on how to ensure work device security. [10] Additionally, 53% of employees say their company has not provided new guidelines for managing sensitive personally identifiable information (PII). [10] This is especially important because some legislation, such as the General Data Protection Regulation (GDPR), requires strict management of data storage locations.

Due to using a personal network when working from home, if malware infects a home network it could spread and end up infecting the organization’s network as well. [11] The number of home networks now connecting greatly expands this threat. Ensuring there are anti-malware controls installed on devices helps mitigate this threat. Current literature does not provide examples of organizations limiting employees from working at locations other than their home office. Working from locations other than the home office could expose more malicious networks to work devices. Additionally, the frequency of which employees connect to other people’s networks for work is also unknown. By allowing employees to work anywhere other than their home, organizations expose themselves to the risks of additional untrusted networks. Organizations should evaluate if the risk is great enough to implement a policy restricting where remote work is allowed.

Another threat of note is regarding privacy concerns. With the popularity of smart-home devices (e.g. Alexa, Google Home) many people have a device constantly listening to them, including when they are discussing sensitive work information. Some organizations may not be comfortable knowing various third parties could be collecting data on their employees’ work conversations. One U.K. law firm required during the pandemic that employees disable their smart home devices and remove them from the work room so sensitive conversations cannot be listened to. [12] Current literature is not clear on how widespread this requirement may be. Additionally, one would think the concern of smart devices listening would apply to cellphones as well, but current literature does not provide examples of organizations limiting this as a result work from home changes. Organizations should evaluate the risk of third parties listening through devices like smart speakers and cellphones to determine if these devices should be limited in work environments.

**Types of Devices Connecting to the Network**

Due to COVID-19, the personal computer (PC) market suffered a 12.3% decline in shipments in the first quarter (Q1) of 2020 compared to Q1 2019. [13] This was the largest decline in this market since 2013. [13] The pandemic caused supply chain disruptions, especially in China, so companies were unable to produce as many computers as normal. [13] There was also a surge in demand for computers because more people were working from home. Since many people suddenly needed to
work from home and there were supply chain problems, organizations were sometimes unable to provide standard corporate owned and managed devices where needed. This resulted in many employees needing to use personal devices for work. This is concerning because corporate owned devices are often much easier to secure than personal devices. [14]

Personal devices used for work are concerning for several reasons. To name a few examples, personal devices may not have standard security software such as endpoint protection programs, they might allow devices plugged in to run malicious executables, and organizations may not have as much visibility into device activity, such as if an employee began saving sensitive data on their personal device. Problems like these can be remediated through making a personal device “managed” by the employer, such as through installing device management software. Time and resources are required to enable an effective managed personal device program.

The previously referenced IBM Security and Morning Consult study found several interesting statistics on personal device use during the pandemic. Discoveries included that 53% of remote employees used personal laptops and computers for work. [10] Sixty-one percent of employees said their employers did not provide tools to secure those personal devices, such as endpoint protection software. [10] Fifty-three percent of those surveyed say their personal devices used for work were not administered at all by their employer. [10] Some good news is that those working with PII were more likely to have their personal devices administered by an employer, likely due to the importance of securing sensitive information. [10] From the above we see that many employees did not use a managed corporate device for work during the pandemic, but something not addressed in the existing literature is if organizations were able to provide corporate devices to employees who did not have them before COVID-19.

**Types of Remote Access**

There are various means available to connect to organization resources remotely for work. Historically, the most common option was to use a virtual private network (VPN), which has been relied upon for over the past 20 years. [15] Due to their architectural design, VPNs can be slow for end users, especially when organizations previously only had a small subset of their employees using them. [15] For VPNs, “the only way to effectively increase capacity was to add equipment”, which is costly and not easy to do quickly. [16] VPNs are becoming a legacy remote access technology.

The main alternatives to VPNs are zero trust network access (ZTNA) solutions and virtual desktop infrastructure (VDI), although other solutions exist as well. VDIs run hosted virtualized desktop environments which can be internet accessible. This allows access to an organization’s internal resources through the remote desktop environment. VDIs may not be as efficient as VPN since they add an additional barrier between the employee and organization resources. VDIs are more useful as dedicated environments with pre-installed resources or greater computing power than just as a remote access tool.

The zero-trust model enforces that access is denied until a user sufficiently proves their identity, hence “zero trust.” With ZTNA, information such as application, location, device, network, or other elements can work together to verify a user’s identity, which can provide for greater security. [16] Zero-trust networks allow users to make a secure connection to a specific resource, including cloud based and on-premise. ZTNAs are a “more flexible alternative to VPNs” which still protect traffic from attackers while offering scalability for the network. [17] Prior to the coronavirus, estimates showed that by 2023, 60% of enterprises will phase out their VPNs in favor of ZTNA. [17]

It is worth noting that remote access solutions are not required to access organization resources from the internet, such as software as a service (SaaS) solutions like Office 365 or Salesforce. This access can be secured through means like a cloud access security broker (CASB). CASBs give organizations greater visibility and control over resources that are in other cloud environments, which is a gap for VPNs. [16] While CASBs provide secure access to cloud-based resources, they do not provide remote access and cannot access on-premise datacenters.

Organizations that require solutions to access their internal networks should look at solutions like ZTNA, VPN, and VDI. Organizations need to evaluate what is best for them, because each of these solutions have different benefits, setup difficulty, and ongoing management needs. Most organizations must consider these options, because in 2019, survey results found 98% of businesses ran server hardware in an on-premise environment. [18]

Existing literature is unclear on how usage of remote access tooling options changed as a result of the pandemic. Because remote access tools were new to people beginning work-from-home, did organizations chose to relax security controls to be more accessible to all employees? For example, did organizations decrease frequency for initial authentication or multifactor authentication (MFA)? Were controls weakened to ease impact on technology like VPNs, by organizations externalizing internal resources? Or could controls have strengthened by choosing to migrate to better, modern solutions? Another major gap includes employee personal reflections of how their employers dealt with cybersecurity as a result of COVID-19. For example, did rushed out telecommunication tools like Zoom make employees feel concerned about the organization’s cybersecurity? Please look forward to part 2 of this series, where I present survey results which address some of the gaps identified in this research.

**Threat Actor Tactics**

Cyber threat actors took advantage of the chaos brought on by COVID-19 in attempts to exploit organizations. Microsoft claims there was not a surge in the overall quantity of cyber-attacks, but rather, the tactics used by threat actors changed given the introduction of COVID-19. [18] While the number of attacks has not significantly changed, Microsoft found that there were more successful attacks, especially in countries which had serious virus outbreaks. [18] Cybersecurity company Zscaler found a rise in COVID-19 related attacks from just...
1,200 in January 2020 to 380,000 in March 2020. [20] Attacks were generally more successful due to fear and desire for new information. [18] Attackers achieving greater success further shows that organizations were unprepared for the pandemic and the ensuing changes. We will now explore some documented examples of COVID-19 enabled or themed attacks, primarily focusing on a study by Lallie et al., which documented information about public coronavirus related attacks. [21]

**Cyber-enabled Crime**

Of the cyber-attacks and campaigns in the Lallie et al. study, 86% of them included phishing. [21] Phishing is an extremely common tactic which preys upon human emotions to illicit responses, such as installing malware or sharing sensitive information. These scams targeted victims with lures like selling goods in high demand (e.g. masks, testing kits) and impersonating organizations such as the World Health Organization. [21] Some scams even used CAPTCHA to appear more legitimate and avoid detection from security crawlers. [20] Some recent phishing scams targeted government COVID-19 stimulus checks and vaccine distribution.

There were six pharming attacks documented in the Lallie et al. timeline. [21] Pharming is when a fake website is set up to appear legitimate. When unsuspecting users enter information, such as credentials, the information is sent to attackers. One large pharming campaign used a fake Office 365 login for access to a fake COVID-19 financial compensation website. [18]

**Cyber-dependent Crime**

The Cyber & Infrastructure Security Agency (CISA) says that threat actors are “taking advantage of this mass move to telework” by exploiting vulnerabilities in popular software used for working from home. [22] For example, remote access tools and communication tools were exploited. [22] There was an increase in attacking insecure remote desktop protocol (RDP) endpoints as well. [22] The Lallie et al. study also found two COVID-19 hacking targets where attackers attempted to steal research on the virus. [21]

The Lallie et al. COVID-19 cyber-attack timeline found 65% of attacks involved malware. [21] Some common malware types included the “Agent Tesla” keylogger and Trojans like “Grace-Wire” and “TrickBot.” [22] These Trojans install other malicious files, like Remote Access Trojans (RATs), desktop sharing clients, and ransomware. [22] Cybercriminals also developed fake VPN software that would install malware when downloaded. [20] Another malware example was a fake Android app for coronavirus tracking that, when installed, would download ransomware and demand payment to unlock the device. [20]

The Lallie et al. COVID-19 cyber-attack timeline found two distributed denial of service (DDoS) attacks, which targeted the U.S. Health Agency and a Chinese epidemic prevention unit. [21] Compared to the second quarter in 2019, security firm Kaspersky found a 217% increase in DDoS attack attempts during the second quarter of 2020, which they believe to be related to the coronavirus. [23] They found that the U.S. and China were victims of the most DDoS attacks, but most DDoS attacks were also launched from these regions. [23]

**Conclusion**

Because of the sudden shift to get employees to work from home, changes were made which posed cybersecurity risks. Organizations need to ensure their IT departments consider cybersecurity throughout an agile development processes, and cybersecurity programs ought to become more agile to meet business needs while ensuring appropriate security. Attackers will continue to take advantage of our mistakes and deliberation, so we need to remain diligent. We must continually evaluate and implement best practices for remote work cybersecurity, especially due to the changes made because of the COVID-19 pandemic.

**About the Author**

Author Douglas Shuman has about five years of experience working in cybersecurity, primarily as a cyber risk analyst. He recently completed his master’s degree in Cybersecurity Analytics and Operations from Penn State University and is certified in Open Factor Analysis of Information Risk (FAIR). His focuses are on cyber risk assessments and cybersecurity consultation. He can be reached at his LinkedIn page.

**References**

COVID-19’s Impact on Organizational Cybersecurity Posture | Douglas Shuman


Members Join ISSA to:
- Earn CPEs through Conferences and Education
- Network with Industry Leaders
- Advance their Careers
- Attend Chapter Events to Meet Local Colleagues
- Become part of Special Interest Groups (SIGs) that focus on particular topics

Join Today: www.issa.org/join

Regular Membership $95* (Includes Quarterly Forums)

CISO Executive Membership $995 (Includes Quarterly Forums)

*US Dollars / Year