The Effect of COVID-19 on Remote Work Policies

Patrick M. Damon, II
Northcentral University, San Diego, California, USA
New York Genome Center, New York, New York, USA

https://doi.org/10.38126/JSPG210101

Corresponding author: pdamon@nygenome.org

Keywords: COVID-19; information security; policy; mobile device management (MDM)

Executive Summary: The climate for information security has drastically shifted due to the COVID-19 pandemic. In the past, information security focused on the purview of the office space and the physical infrastructure, with increased specializations in digital architecture such as the Internet of Things, cloud services, and Software-as-a-Service (SaaS). Remote work was often discouraged due to ineffective mitigation strategies, especially when personal devices were involved. Remote work has become commonplace, and information security specialists must adapt to the changing environment. Effective information security policy management for a modern age will include effective mobile and remote usage provisions that maintain the same or similar workflow as on-site activities. Virtualization offers enhanced security for remote work while maintaining set routines.

I. COVID-19 & Information Security

Prior to the advent of COVID-19, only six percent of employed individuals worked from home a majority of the time, while three-fourths of all workers had never worked remotely (Coate 2021). Early in 2020, the world was thrown into chaos as the recognition of a new virus swept across nations, effectively grinding the standard of work to a halt to preserve human life. Slowly, work resumed, but in diminished and, in most fields that were able to do so, remote capacity. By late spring of 2020, over a third of employed individuals were working from home (Coate 2021). With this shift in work practice came created vulnerabilities in remote work schemes. Some countries saw a nearly 300% rise in cyberattacks within 2020 alone (National Cyber Security Centre 2020). In 2019 there were a reported 1,473 data breaches, while in the first third of 2020 alone, there was a globally reported 2,953 breaches (Jay 2022; Purplesec 2021).

Though more research needs to be conducted to determine the exact cause of the increase, it is clear that malefactors are leveraging the shift in working dynamic due to COVID-19 to double down on their attempts at malicious activity, especially in the area of social engineering (Jay 2022; National Cyber Security Centre 2020; Purplesec 2021).

There are several possible factors as to why these incidents increased. The first is that people, on the whole, have been able to spend more time at home with fewer options for effective network traffic supervision due to the increased reliance on personal devices, and those users without formal information technology training may not be aware of what signs to look for to determine breaches on their home network. Additionally, information security programs have traditionally relied on in-person information tactics such as posters and other forms of visual media to create social deterrents and reminders, which do not exist in home environments. Furthermore, COVID-specific threats arose, such as spoofed domains that were made to look legitimate with coronavirus buzzwords appearing in search engine results and offering malware and ransomware instead of safety and security. Online scams and phishing attempts have skyrocketed with over one million COVID-19 linked falsified messages, sowing discord and misinformation as the world attempts to correct its course (Interpol 2020).

As the world shifted from being reliant on away-from-the-home work sites, data trends show that a fourth of all jobs in the United States will likely be remote by the end of 2022 (Robinson 2022). Though this may be good for the work-life balance, it poses considerable concerns for information security in all sizes and shapes of business. The workplace, as it was known, has wholly changed. Even if a return to in-person work is made en masse, the impact of COVID-19 on how information security is handled is extreme.

II. Remote Work Challenges

Confidentiality, integrity, and availability are ingrained in the core of information security practices, but how well do they apply when the traditional office network infrastructure has become decentralized in favor of home networks? Traditional network lifecycles involve routinely upgrading and hardening assets within the network infrastructure to ensure the security of the data housed by the organization. As technology has innovated, the number of access points available to modern office infrastructure has increased. For example, public wireless networks allowed guests to access office internet, which ultimately led to a best practice of developing the network infrastructure to have public and private networks. Developing effective infrastructure for remote work is necessary, but can be difficult due to the decentralized nature of mobile work. As such, effective policy will be critical in mitigating cyber threats that will seek to take advantage of the changing paradigm.

There are several challenges to examine to effectively and securely build and maintain a remote work technology policy. These include:

- How to securely connect to the infrastructure
- How to ensure that personal devices used with the infrastructure are secure and free of malware
- How to mitigate breaches on personal devices
- How to manage potential conflicts of technological interfacing between older and newer products
- How to handle data ownership concerns on infected personal devices
- How to effectively implement remote access controls

Providing the organization in question allows for personal devices to be used, remote work has increased the overall comfort capacity for workers, and they can use systems and setups that work best for them (Cybersecurity and Infrastructure Security Agency 2021). This setup favors most organizations since it reduces the costs of materials necessary to maintain day-to-day operations. While devices may allow for separate work profiles to be created, there can still be a conflict with employees on what can be done to the data on their devices (Cybersecurity and Infrastructure Security Agency 2021). For example, a research institution may have reservations about remotely wiping a stolen device that has both institutional data and data that is proprietary to the researcher.

III. Policy Considerations

Innovation-oriented companies should see the need to develop an effective remote policy and balance how to manage work data while having minimal impact on personal data. If the policies fail to address personal data sovereignty, it will inevitably lead to conflict with users. It would be simple for a policy to have employees sign documents allowing for remote wiping of personal devices that contain organizational data. However, doing so would erode any relationship of trust between the organization and its employees.

Data ownership across non-organizational devices is not a new challenge. Mobile device management (MDM) programs often allow remote wipe devices. Usually, such a feature is reserved for scenarios where a device is lost, stolen, or a threat is discovered. However, wiping an entire device not only removes the company-owned data but any personal data as well. MDM programs are new in the scheme of things, and before COVID-19, this risk was much more acceptable because personal devices could be banned from work use.

Effective remote work policies would include the four primary considerations:

i. Infrastructure

The first consideration includes determining how to maximize infrastructure and minimize access points. When designing policies for remote work conditions on an information technology scale, it is necessary to spin an interconnected web with multiple fail points—much like in networks designed around the Internet of Things (IoT). IoT devices are those that interface directly with each other to circumvent the need for a 'middle-person' to operate each device. For example, a smart refrigerator may send an alert to the networked smart home that the milk has gone bad, which in turn pushes a notification to its user's phone. Utilizing multiple nodes that can interface together is vastly superior to a centralized system. If one node fails, the rest can pick up the slack. A compelling example of this is the utilization of virtual modules.

A virtual node that entities could connect through with appropriate credentials could act as a security checkpoint to protect the central network. If a node is recognized to have its policies violated, the system drops the virtual node and spins a new instance. In other words, creating a bubble that houses all of the necessary components for a user to do their job that will pop and reform if certain rules are met or violated, protecting the central network from being affected by potentially malicious events. The isolation of applications and machines provides an additional security benefit in the event of virtual node infection (Rawal 2020).

ii. Effective Virtualization

The second consideration revolves around how to virtualize the work process effectively. Creating virtualization policies will give the user a window into the system they would utilize if they were in person. Virtualization, in this context, is the process of creating artificial environments that act as sandboxes with all of the programs a user would need to achieve their work goals, remotely accessed using authorized credentials. The virtualization can act as a buffer zone between the user's personal device and the network proper. There is unique flexibility that the virtualization process can offer remote work concepts. One such improvement would be a reduction in necessary hardware that must be maintained. If workers are not in an office environment, it does not make sense to maintain the hardware that would fit that purpose. It would be possible to reduce the overall physical security risk by removing the hardware and allowing the software to exist within virtual space (Rawal 2020). This adjustment effectively reduces physical maintenance times to a fraction of what was previously necessary.

iii. Data Handling

The third consideration involves determining how data will be handled in the event of an incident. The virtualization process also reduces the impact on the organization if a personal device becomes infected with malware or otherwise compromised. The protection primarily covers the organization, but the virtualization window also prevents the user from potentially losing personal data in a remote wipe. No organizational data would be stored locally by enacting a policy that restricts data creation to the virtual environment. For example, if a personal device flags the policy ruleset, its connection will be dropped until all policies can be adhered to.

iv. Training Considerations

Effective training plans balance mitigating day-to-day business with meeting applicable guidelines and standards. The best way to facilitate remote work situations is to reduce the change the user must go through to complete the same tasks they would do in person. Virtualization is an effective tool for this, considering the program works as though they were accessing a terminal on-site.

One critical consideration for remote work information security training is the lack of physical reminders for personnel. An effective security team utilizing a virtualized environment will engage the organization in developing a culture of cybersecurity. It is prudent to train on a more regular schedule following best practices. A hands-on approach will develop a conversation of security that is often replaced with media in physical environments (Birkinsha, Gudka, and D'Amato 2021).

Finally, the security training program for remote work must have provisions for effective communication. The user must know when and who to communicate to and feel confident that the security policies are protecting them as much as the organization. Developing trust between the users and the cyber and information security teams is critical for an effective remote work policy. There is a unique opportunity to turn the user, most often considered the weakest in the security chain, into a living detection asset (Albedrop, Sanchez, and Skootsky 2021).

V. Conclusion

The pandemic has undoubtedly changed how information technology will engage in the workplace. Thus, it is necessary to innovate the mindset of policy building for security. Virtualization offers a unique opportunity to facilitate continued remote work and develop secure systems. The coming years will show an evolution in security concepts and policy creation that will protect the organization and the user in an expanding and changing workplace environment.

References

Albedrop, Sanchez, and Tamara Skootsky. 2021. "Navigating the Expansion of Virtual Communication at Work." *TIP: The Industrial-Organizational Psychologist* 59(1):1–10. https://www.siop.org/Research-Publications/Items-of-Interest/ArtMID/19366/ArticleID/5245/Navigating-the-Expansion-of-Virtual-Communication-at-Work.

Birkinshaw, Gudka, and Vittorio D'Amato. 2021. "The Blinkered Boss: How has Managerial Behavior Changed with the Shift to Virtual Working?" *California Management Review* 63,(4):5–26. https://doi.org/10.1177/00081256211025823.

Coate, Patrick. 2021. "Remote Work Before, During, and after the Pandemic." *NCCI*. January 25, 2021. https://www.ncci.com/SecureDocuments/QEB/QEB_Q4_2020_RemoteWork.html.

Cybersecurity and Infrastructure Security Agency. 2021. "Selecting and Hardening Remote Access VPN Solutions." *Department of Defense.* https://media.defense.gov/2021/Sep/28/2002863184/-1/-1/0/CSI_SELECTING-HARDENING-REMOTE-ACCESS-VPNS-20210928.PDF.

Interpol. 2021. "COVID-19 Cyberthreats." https://www.interpol.int/en/Crimes/Cybercrime/COVID-19-cyberthreats.

Jay, Allan. 2022. "73 Important Cybercrime Statistics: 2021/2022 Data Analysis and Projections." *FinancesOnline.* https://financesonline.com/cybercrime-statistics/.

National Cyber Security Centre. 2020. "Jump in Cyber Attacks During Covid-19 Confinement." https://www.swissinfo.ch/eng/jump-in-cyber-attacks-during-covid-19-confinement/45818794.

PurpleSec. 2021. "Cyber security statistics: The Ultimate List of Stats, Data and Trends." https://purplesec.us/resources/cyber-security-statistics/.

Rawal, Pratyaksha. 2020 "Virtualization Gains Popularity as a Viable Solution for Enhancing Cloud Security." https://cloudlytics.com/virtualization-gains-popularity-as-a-viable-solution-for-enhancing-cloud-security/.

Robinson, Bryan. 2022 "Remote Work Is Here to Stay and Will Increase into 2023, Experts Say." *Forbes.* https://www.forbes.com/sites/bryanrobinson/2022/02/01/remote-work-is-here-to-stay-and-will-increase-into-2023-experts-say/?sh=61bce35c20a6.

Patrick M. Damon, II (they/them/theirs) is an Information Security Analyst specializing in policy building, SOP development, incident response, and security culture development. They received their B.A. in Sociology from Fordham University in 2013 and served for 6 years as a Sonar Technician for the US Navy. They received their Masters in Cybersecurity Tech from UMGC in 2019 and are presently a doctoral candidate at Northcentral University. Patrick is a trans, non-binary, queer individual and was the first uniformed service member to march in the NYC Pride Parade in 2017.

Acknowledgements
I thank Dr. Lyn Lazar and Dr. Frank Appunn for their support and continued guidance through my research.