

# COVID-19 Warrants Modified Cybersecurity for Work-At-Home

Many privacy and data protection statutes require businesses to implement “reasonable security procedures” to protect personal information. See, e.g., Cal. Civ. Code § 1798.81.5 (requiring businesses that own, license, or maintain personal information about a California resident to implement and maintain reasonable security procedures and practices appropriate to the nature of the information).

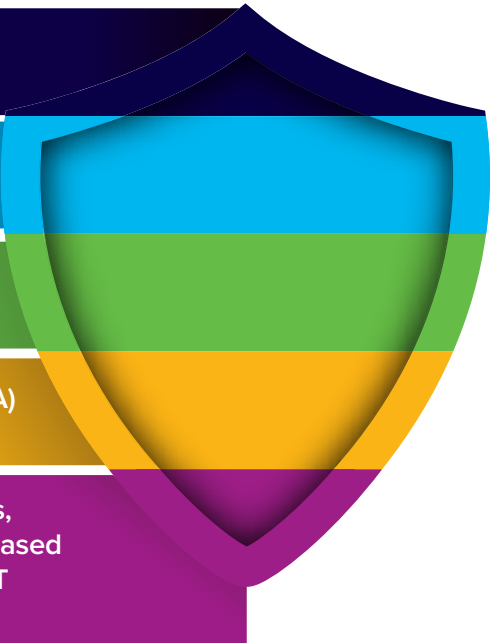
“Reasonable security procedures” is undefined as what is “reasonable” depends on the size of each business and the nature of the data collected. As a result, many organizations rely on guidelines and frameworks when making decisions (e.g., NIST Cybersecurity Framework, Top 20 CIS Controls, etc.). Notably, the California Attorney General has even provided its view that the Top 20 CIS Controls represent the “minimum level of information security that all organizations that collect or maintain personal information should meet,” which

suggests that such controls represent the baseline for “reasonable security procedures and practices,” at least in California. See California Data Breach Report at p. 30, available at <https://oag.ca.gov/breachreport2016>.

However, as coronavirus (COVID-19) continues to spread and businesses worldwide are forced to shift abruptly to a work-at-home workforce, the question arises as to whether the standard for “reasonable security” changes. While many businesses had continuity plans, the plans often assumed that crisis would be limited in geography (e.g., shifting operations after a hurricane from Florida to Iowa). Despite the fact that many organizations likely did not prepare for global pandemic, the regulatory and agency guidance issued thus far seem to lead us to the same conclusion: COVID-19 warrants a shift in cybersecurity practices.

---

On March 13, 2020, the Cybersecurity and Infrastructure Security Agency (CISA) released an [alert](#) encouraging organizations to adopt a “heightened state of cybersecurity” when considering remote work options. CISA specifically noted the following risks introduced by work-at-home:

- 
1. As organizations use VPNs for telework, more vulnerabilities are being found and targeted by malicious cyber actors.
  2. As VPNs are 24/7, organizations are less likely to roll out the latest security updates and patches.
  3. Malicious cyber actors may increase phishing emails targeting teleworkers to steal their usernames and passwords.
  4. Organizations that do not use multi-factor authentication (MFA) for remote access are more susceptible to phishing attacks.
  5. Organizations may have a limited number of VPN connections, after which point no other employee can telework. With decreased availability, critical business operations may suffer, including IT security personnel’s ability to perform cybersecurity tasks.

In addition to CISA, the U.S. Department of Health and Human Services (HHS) is reminding entities to maintain “reasonable safeguards,” with no indication that such safeguards are relaxed during a time of crisis. Indeed, on February 2, 2020, the HHS issued the [HIPAA Privacy and Novel Coronavirus Bulletin](#), which provided that even in emergency situations, covered entities must continue to implement reasonable safeguards and must apply the administrative, physical, and technical safeguards of the HIPAA Security Rule to electronic protected health information.

On March 1, 2020, the HHS issued the [HIPAA and COVID-19 Bulletin](#), which provided that sanctions and penalties against covered hospitals that did not comply with certain provisions of the HIPAA Privacy Rule would be waived. This limited waiver, however, did not change or relax the requirements to safeguard patient information. Instead, the bulletin again reminded covered entities that even in emergency situations, reasonable safeguards must be intact.

On March 10, 2020, the New York Department of Financial Services (DFS) issued its own [guidance](#) and requested assurances from covered entities of their “operational preparedness” to address risks posed by COVID-19. Specifically, the DFS is requiring all covered institutions to submit a response to the DFS describing the institution’s plan of preparedness to manage the risk of disruption to its services and operations. The plan must include an assessment of potential increased cyber-attacks and fraud and an assessment and testing of the capacity of the existing information technology and systems in light of a potential increased remote usage.

Notably, the DFS is one of the few regulatory bodies that prescribes specific requirements for a “cybersecurity program” that all covered institutions must adopt. See 23 NYCRR 500. The March 10th guidance does not suggest that such requirements are relaxed or will not be enforced in light of COVID-19.

Rather, the DFS’ request for assurances suggests that such requirements matter now, more than ever before.

From a practical perspective, businesses need to give heed to the various alerts and guidance issued on cybersecurity in the wake of COVID-19 and consider what safeguards need to be implemented to address the potential effects and risks of the COVID-19 outbreak. To that end, businesses should constantly evaluate the circumstances and build now a plan that addresses the impact of the outbreak in stages (e.g., 30-60-90-120-180 days) documenting the lessons and reasons for making modifications over the same intervals. Businesses would be wise to create a plan bearing the end in mind when things return back to “normal” so that efforts can be appropriately scaled, consistent with the effects of a particular stage, and then appropriately clawed back, when needed.

Given how quickly new practices and procedures are being rolled out, businesses should also consider creating a “COVID-19 Resource Center” to document the new, but likely temporary, notices, policies, and procedures. Not only will this allow employees to reference any new policies, as need be, but it will allow the organization to keep track of what policies have been implemented and changed during this period of time. Such a tool can also be effective in maintaining a controlled and documented vendor management plan as well.

In terms of physical, security, and administrative safeguards, below are a few measures to consider as businesses worldwide shift to remote work:

1. Assessing potential increased risks of cyber-attacks made possible by the scale of the work-from-home population.
2. Assessing the preparedness of critical outside-party service providers and suppliers. At a minimum, consider requiring critical vendors to submit assurances within a fixed period of time of their operational preparedness to address the effects of the COVID-19 outbreak.
3. Implementing multi-factor authentication (MFA) on all VPN connections to increase security. If MFA is not implemented, require remote workers to use strong passwords.
4. Updating VPNs, network infrastructure devices, and devices being used to remote into work environments with the latest software patches and security configurations.
5. Providing a list of measures to improve or enhance home security (e.g., secure router, unique user ID that are not shared with others in household).
6. Reiterating the importance of the “clean desk” policy, even when working from home.
7. Raising employee awareness to the increased risk of cyberattacks including, specifically, phishing scams.
8. Issuing company devices, where possible, and avoiding the use of personal devices for remote work even if using a sandbox (e.g., Citrix).
9. Distributing information security tools virtually (e.g., antivirus and anti-malware software) and ensuring updates occur in a controller manner.
10. Assessing risks of information storage and disposal, which will be most prevalent if paper files are being brought home or if information is being stored locally or on portable devices.
11. Requiring employees to use only encrypted communications (e.g., no personal email even when VPN is down).
12. Requiring authentication before receiving calls from helpdesks or otherwise to avoid pretexting/phishing.
13. Ensuring incident response plans are up to date (e.g., virtual workspace contact information for CIRT members and backup contacts) and ensuring IT security personnel are prepared to ramp up the following remote access cybersecurity tasks: log review, attack detection, and incident response and recovery.
14. Ensuring IT security personnel test VPN limitations to prepare for mass usage and, if possible, implement modifications—such as rate limiting—to prioritize users that will require higher bandwidths.
15. Reviewing cyber-insurance to determine what is covered. Policies should be broad enough to cover incidents that may occur while employees are working from home.

COVID-19 and work-at-home mandates create new challenges for all of us. We expect criminals to take advantage of this crisis. Together, we can work to limit business disruption without compromising privacy or security. Doing so requires us to confront the new reality of doing business in the midst of COVID-19 and planning for what comes after. We will continue to monitor guidance coming from the policy makers and provide further information and updates so that we can continue the dialogue.



**Ronald I. Raether, Jr.**

[ron.raether@troutman.com](mailto:ron.raether@troutman.com)

Ron leads the Cybersecurity, Information Governance and Privacy practice group at Troutman Sanders. He is known as the interpreter between businesses and information technology and has assisted companies in navigating privacy and data security laws for over 20 years, defending hundreds of putative class actions making privacy and data security-based claims.



**Sadia Mirza**

[sadia.mirza@troutman.com](mailto:sadia.mirza@troutman.com)

Sadia is a Certified Information Privacy Professional in the United States (CIPP/US) and a Certified Information Privacy Manager (CIPM). She has extensive experience in data security and privacy matters, having handled a number of data breaches and investigations in a variety of industries.