How the ARM Industry Can Maintain Security and Compliance While Working from Home

By Andrew House

This article is an excerpt from the Fall 2021 RMAI Insights *magazine (pages 12, 28, 29 and 30), originally published October 15, 2021.*

With the emergence of new technologies, paired with reliable and widely accessible Internet access, personal electronic devices can now effectively communicate from almost anywhere in the world. Paired with the current global pandemic, we've reached a point where working from home no longer inhibits productivity and, in many industries, can become the new normal in order to maintain an employee workforce large enough to satisfy our industry's demand.

As we move toward this new work-from-home standard, some states like Minnesota and Connecticut have already begun creating their own individual guidelines. Prior to moving too far forward in this direction as an industry, it would be a best practice to create and present some universal standards that can be agreed upon now before continued state guideline variances continue to form.

Similar to what we're seeing unfold with state-specific consumer protection laws (California's CCPA, Colorado Privacy Act, Nevada's AB 323 and SB 260 bills, Texas' HB 3741, West Virginia's HB 3159, and Florida's HB 969), it will be extremely difficult for any organization that operates across multiple state lines to keep track of yet another subset of state-specific guidelines.

There are several facets to consider when implementing some type of universal work from home guidelines. Data security and compliance are the clear frontrunners in both complexity and cost of implementation, specifically for those organizations utilizing outdated or legacy systems that aren't capable of handling remote worker bandwidth.

The best next step should be creating a standardized set of guidelines utilizing a few industry standards that have already been widely accepted, including but not limited to PCI DSS, SOC 2, and HIPAA. Rather than attempting to reinvent the wheel, we need to pair these standards with an instillment of trust in our remote employee workforce while also creating a set of compensating controls so the security and compliance standards that we've all worked so hard to create and maintain don't have to suffer.

That being said, the chances of all states coming together in unity are extremely low. Instead, let's review some specific controls that should be the most prevalent across the country to be better prepared as additional state-specific guidelines continue to be formed.

Security

CISA - https://www.cisa.gov/telework
CIS - https://www.cisecurity.org/blog/how-cis-can-help-teleworkers-improve-their-cyber-defenses/
NIST - https://csrc.nist.gov/projects/telework-working-anytime-anywhere

In addition to more comprehensive security controls and resources from reputable organizations like the ones mentioned above, I've outlined below a few of my high level "musts" when creating a work-from-home technology plan.

Principles of Least Privileged Permissions

The first step, before doing anything, is to determine the work-from-home scope. Using job descriptions or other applicable task lists, create a list of the work-from-home employees and determine the very lowest access level an employee could receive without affecting their performance. This first step is imperative to creating the necessary security controls and properly justifying access to any company information or resources.

The Benefits of Connecting via Company Issued Device

Work-from-home employees should always be utilizing some type of standardized company equipment. Not only does this make it easier on internal technical resources when troubleshooting issues remotely, but device management and configuration becomes much more uniform and simplified. It will also be critical in preventing data leakage when properly configured.

Ideally, these company owned devices should be thin clients. When powered on, a thin client will look and perform very similar to a standard out of the box laptop but from a security standpoint is a far better solution. The thin client typically contains no local hard drive and instead relies on securely connecting to the company network to obtain all work-related documents, sensitive data, memory and applications. This prevents company data from being saved on devices that have a higher risk of being compromised than those inside a secure company facility. With this secured login layer in place preventing unauthorized access to company data, many of the in-office security control requirements such as CCTV cameras, 24/7/365 security guards and facility keycard or similar access control can be satisfied with a compensating control.

> **“Work-from-home employees should always be utilizing some type of standardized company equipment.”**

The thin client device should connect to the network in a way that keeps it protected by company firewalls as if the employee were still in the office. Many best practice firewall configurations limit websites that can be visited by blocking website categories such as Chat/Instant Messaging, Hacking, Malware and Freeware/Software Downloads. In addition to web category restrictions, specific port blocking or whitelisting through the firewall can also assist with preventing the work-from -home users from accessing FTP/SFTP sites where large amounts of data could be uploaded to unknown sources or locations. Again, the items being restricted go back to the scope of work being performed and least privileged permission needed, as we discussed earlier.

Creating a Secured Working Environment

After making the decision to utilize a secured thin client, the last step is ensuring the connections to company networks are done securely. As the employee will most likely be utilizing their own personal at-home internet connection, the following configurations are critical to security success.

The thin client should connect using Multi Factor Authentication to prevent unauthorized access to the company network. Multi Factor Authentication is an authentication method that requires two or more pieces of evidence to log-in. (Something the user knows, possesses, or “is”). Common Multi Factor Authentication methods are requiring the user to first enter their username and password, followed by immediately receiving an email or SMS message with a uniquely generated one time password that must be inputted to complete the connection process.

Once connected, ensure the thin client cannot stay connected to the network during long periods of user inactivity. Typically, after a short period of time, such as 5 minutes with no keystrokes entered or mouse pointer movement, the user should be forcefully disconnected from the network to prevent potential unauthorized access to the network. This is a common practice within the office environment but is especially important while working from home when an employee could easily be distracted by non-work-related tasks, such as doing the laundry or loading the dishwasher.

Lastly, ensure that any split tunneling connectivity is disabled. Split tunneling allows a device to decide which data is sent encrypted over the company network versus unencrypted to other sources. Since the thin client’s connection to the office network (VPN) should encrypt the data as it’s sent and received by default, disabling split tunneling will ensure there is no gap in an encrypted electronic communication.

Maintaining Stringent Levels of Compliance

As with data security and privacy, compliance has several factors to consider. Make sure to do your research into your state’s employment rules regarding any potential tax implications if any employees happen to be located outside of state

lines. It would also be an excellent practice to verify your insurance policies, looking for specific coverage on remote workers, data loss, and theft. Having your employees who will be working remotely sign a waiver would also be an extra layer of added protection and security.

It will be extremely important to have a process in place to measure performance metrics. This is somewhat of an unknown in this recently adopted method of service in the receivables space. Maintaining client satisfaction and employee performance levels are necessary and critical in this ever-changing environment. Having open and honest relationships between clients and vendors will make this a win-win situation for everyone involved.

Of course, we cannot forget the regulatory rules along the way. While measuring performance is important, there needs to be a manageable audit process in place to ensure regulatory compliance. IT support will also be vital when it comes to tracking call times and call recordings. These will need to be easily and readily accessible.

Another item on the checklist should be remote employee waivers. These will cover a plethora of elements and will need to align with the company's expectations. Items to be addressed will be the remote workspace expectations and applicable privacy rules to name just a couple. One new and modern hurdle to overcome will be the emergence of recordable devices such as Alexa, Google Dot, etc. This creates a new dimension of potential issues. Employees should be in a quiet and private work space any time they are making calls or accessing sensitive information with all unnecessary devices turned completely off and inactive. These waivers should be signed by the employee, countersigned by a corresponding manager, and kept with the employee's file to be reviewed and re-signed yearly, or more frequently as applicable regulatory and/ or security changes are made to your work-from-home guidelines.

Ultimately, while it is unlikely that all states will adopt such comprehensive and universal security and compliance requirements, the aforementioned suggestions and guidance should help organizations create a solid foundation that can be built upon for states that attempt to create overreaching work-from-home guidelines.

Andrew House
Chief Security Officer
VeriFacts, LLC

Andrew House is one of four owners of the Women Owned Small Business, VeriFacts, LLC and holds the title of Chief Security Officer. He has been with VeriFacts since 2006 and his primary focus is the oversight of IT, Vendor Management, and R&D divisions with an emphasis on software development, process improvement and the implementation of emerging technologies.