Published on *The National Law Review* https://natlawreview.com

COVID-19 & Cybersecurity: What Companies and Employees Should Know About Remote Working

Article By:

Peter Baldwin

Jason G. Weiss

The spread of COVID-19 has prompted an enormous shift by organizations to the use and implementation of remote working solutions for a wide range and number of employees. Unfortunately – but perhaps not surprisingly – this shift has provided malicious cyber actors with additional ways to infiltrate remote use networks. The spread of COVID-19 has brought with it a huge surge in data security incidents, as hackers look to exploit new organizational vulnerabilities and distracted and overburdened IT security personnel.

It is understandable that most employees may not have cybersecurity at the forefront of their minds at this time. However, malicious actors have sought and inevitably will continue to seek to exploit the fact that employees – and especially those employees who are new to remote working solutions – currently are less observant about detecting cyber-attacks. Attempted attacks have targeted organizations across all industries, and COVID-19-related cyber-attacks have included, among others, email phishing and business email compromise (BEC) scams. Thus, it is critical for organizations to recognize the current threat environment and maintain an enhanced focus on cyber defense.

In an attempt to assist organizations, the United States Cyber and Infrastructure Security Agency (CISA) recently issued an alert highlighting key cybersecurity considerations and defensive steps that organizations can take to prepare for and combat the rise in cyber threats seeking to exploit remote working solutions. CISA's alert advised organizations to be aware of the following potential issues related to remote working:

- As more organizations use virtual private networks (VPNs), more VPN vulnerabilities are being found and targeted by malicious actors
- Organizations traditionally have been less likely to keep VPNs updated with the latest security updates and patches
- Malicious actors are increasing the use of phishing emails targeting remote working employees

- Organizations that do not use multi-factor authentication (MFA) for remote access are particularly susceptible to cyber-attacks
- Organizations may have limited VPN connections, potentially causing critical operations to suffer

In response to these new remote working risk considerations, CISA recommended that organizations take the following steps to protect themselves:

- Regularly update VPNs, network infrastructure devices, and devices used to access systems with the latest software patches and security configurations
- Alert employees to increased phishing attempts and how to prevent these attacks from working
- Ensure IT security personnel are prepared to address remote access security issues
- Implement MFA on all VPN connections – especially for those remotely accessing a network
- Ensure that IP security personnel test VPN limitations and prepare for mass usage
- Contact appropriate law enforcement or regulatory agencies to report cybersecurity incidents or attacks

In a separate alert, CISA also addressed the rise in COVID-19 phishing and scam emails and advised organizations to exercise caution in handling any email with a COVID-19-related subject line, attachment, or hyperlink. CISA further advised that organizations should notify their employees to be wary of social media pleas, texts, or calls purportedly related to COVID-19.

CISA advised organizations to instruct their employees to take the following precautions in order to prevent against victimization by COVID-19 scams:

- Avoid clicking on any links in unsolicited emails and be wary of email attachments
- Use only trusted sources with fact-based information on COVID-19
- Do not reveal personal financial information in email, and do not respond to solicitations for this information
- Independently verify an organization’s authenticity before making a donation

In addition to the foregoing, organizations would be wise to ensure that their cyber incident response plan addresses and contemplates potential issues and concerns arising out of remote working. Moreover, organizations should confirm that their crisis management and incident response plans are executable by a remote workforce – including remote IT personnel.

COVID-19 has caused significant disruption to the operations of most organizations throughout the

country and, in many cases, employees have understandably lost focus on cyber security. Hackers and malicious actors are seeking to exploit this situation. Therefore, it is crucial that, even in these difficult times, all organizations remain vigilant in their cyber defense.

National Law Review, Volume X, Number 86