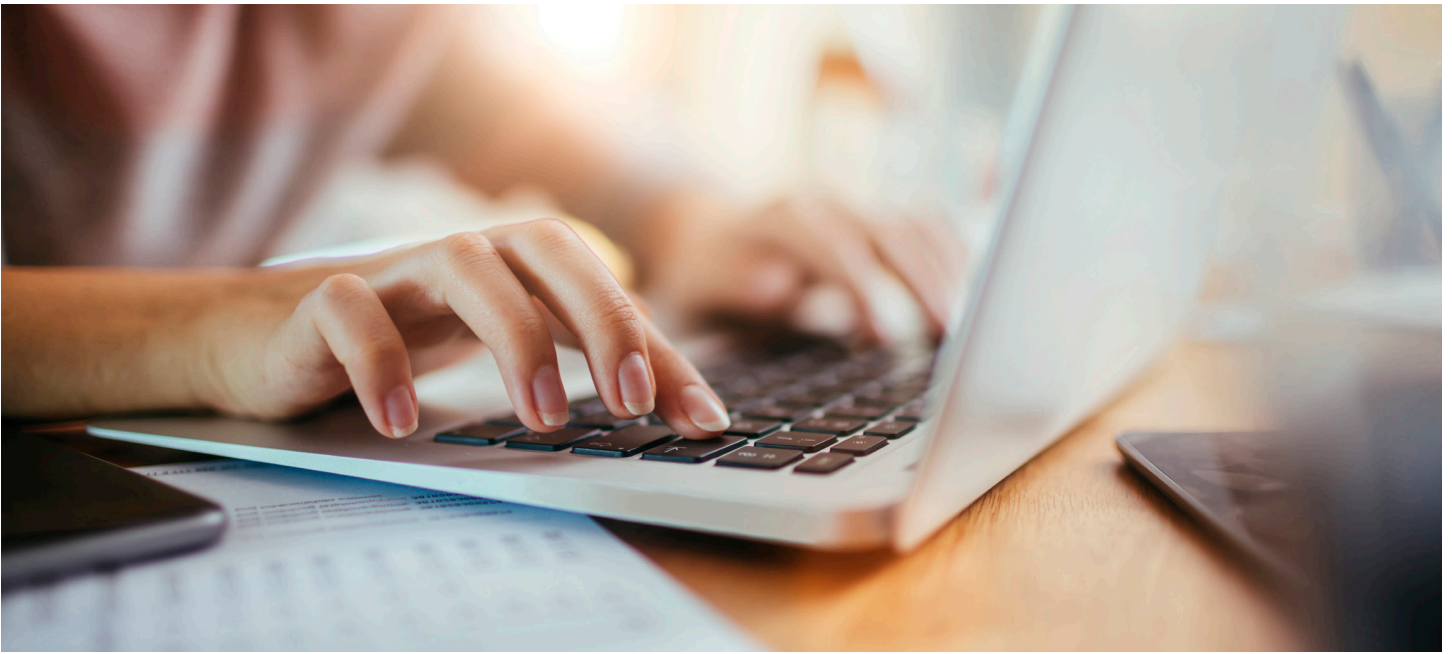


NetDiligence®

**COVID-19:
Rising Cybersecurity
Threats**





COVID-19: Rising Cybersecurity Threats

With the rise of the global pandemic COVID-19, organizations are in many cases forced to transition to a telecommuting workforce. And while technology enables work to continue from a medically safer distance, these new arrangements come with another warning: increased cybersecurity risk.

At the "COVID-19 Emerging Issues: Managing Cyber Risks of a Remote Workforce and Global Privacy Concerns" webinar, presented by NetDiligence and Arete Incident Response on March 24th, Marc Bleicher, managing director at Arete Advisors, highlighted how to safely manage the move from a traditional shared office to the home office.

Among the most obvious lapses are unsecured wi-fi networks, ill-equipped

personal devices and networks, and workers untrained in the nuances of cybersecurity in the home setting.

"The attack surface for the bad actor is wider than ever with more remote connections and remote access solutions," Bleicher said.

The pandemic's lockdown conditions are unlike the typical telecommuters. Many workers have been thrust into this new reality without training or preparation, having never worked from home before. Given the sudden, untraditional work setting and work hours, as well as the additional demands of home-schooling and the emotional toll of stress and uncertainty, employees may be more vulnerable to scams and social engineering.

In addition, bad actors have already begun to exploit COVID-19 with new attacks. Already phishing emails, malicious apps and fake sites designed with the intention to infect users have emerged in the days since the contagion has spread around the world.

"Threat actors are taking advantage of this crisis and especially targeting healthcare companies," Bleicher said. "These organizations and the organizations that support them are at higher risk for attack."

The bottom line: All organizations should be mindful of cybersecurity now more than ever, and those with remote workers should take special care to both ensure the integrity of existing security measures and avoid common pitfalls.



Cultivating Awareness

For everyone, the shift to remote work requires a cultural shift. Employees are accustomed to walking down the hallway to find IT support, Bleicher says. Now IT and information security must find a way to be accessible to workers in their respective homes.

Organizations should review their remote working policies and apprise their employees about cybersecurity procedures. If the policies need to be updated, this is a good time to begin that process.

The defense against cyber events begins with education of the remote workforce and a shared understanding of the challenges

ahead. That process can be divided into three buckets:

- Secure business applications and systems that are now remotely accessible.
- Expect phishing scams, social engineering and other exploits to increase.
- Prepare for the eventual return to the workplace and any security risks that might originate on individual user devices and threaten the enterprise network.

Securing the Organization

First and foremost, organizations should adopt the same cybersecurity hygiene protocol for remote workers as they would in an office setting. In most cases, that means remote workers will be accessing the organization's VPN from home. Remote work environments can pose security issues from multiple angles, whether that's the remote technology used, application access and access controls, or a lack of IT support.

"One of the things we need to be aware of from an IT standpoint is how to accommodate everyone. We all use solutions like Zoom or Team Viewer and these are great for collaborating," Bleicher said. "But we need to be ready for the influx of more connections that naturally occur. Users need to be able to connect in a secure way. IT and information security teams also need to be ready to monitor for antivirus alerts and other evidence of malicious activity."

The good news is that there are immediate steps to better secure the network and applications from the organization side.

1. Enable two-factor authentication.
2. Use VPN only.
3. Restrict and secure internet-facing remote access and management tools.
4. Install advanced endpoint detection and monitoring tools such as SentinelOne or Carbon Black.
5. Regularly update all systems and apply patches where recommended.
6. Disable SMBv1, a known vulnerability in legacy Windows systems.

Securing Remote Workstations

On the employee side, security measures must be implemented at home. Concerns to be mindful of include endpoint protection, password hygiene, RDP system settings, wireless security, patching and updating applications, home system sharing, and unknown applications.

"From a remote worker standpoint, many of the same issues apply. You want to stay connected and updated while staying secure."

General steps employees should take to better protect data and systems at home include:

1. Don't provide personal information, including usernames and passwords.
2. Never click attachments or links in emails without verifying their legitimacy with IT or information security teams.
3. Ensure that WPA2 has been enabled on the Wi-Fi router.
4. Change the default administrator password on all home routers and devices.
5. Allow trusted connections only.
6. Disable SMBv1, a known vulnerability in legacy Windows systems.
7. Ensure all personal devices are current with patches, packs, and system updates.
8. Install antivirus and advanced endpoint security in all personal devices.
9. Never store sensitive or for official use only (FOUO) data on personal devices.

Staying Vigilant

It's critical that organizations and at-home workers stay remain increasingly wary of potential exploits out there, Bleicher said. Given the amount of new activity in connection with COVID-19, there is reason to be concerned. "As a home user, we should use even more caution," he said. "I don't mean to harp on fear, but this is a time when we need to be extra suspicious."

About NetDiligence®

NetDiligence® specializes in Cyber Risk Readiness & Response services. With more than 18 years of experience in cyber, NetDiligence is an award-winning provider of innovative cyber risk management software and services to the insurance industry, including QuietAudit® Cyber Risk Assessments, the eRiskHub® cyber risk management portal, and Breach Plan Connect® software-as-a-service (SaaS) and paired mobile app to help policyholders with data breach response planning. NetDiligence publishes an annual Cyber Claims Study and hosts annual Cyber Risk Summits in Philadelphia, Santa Monica, Toronto, London, and Bermuda. For more information, visit <https://netdiligence.com>.