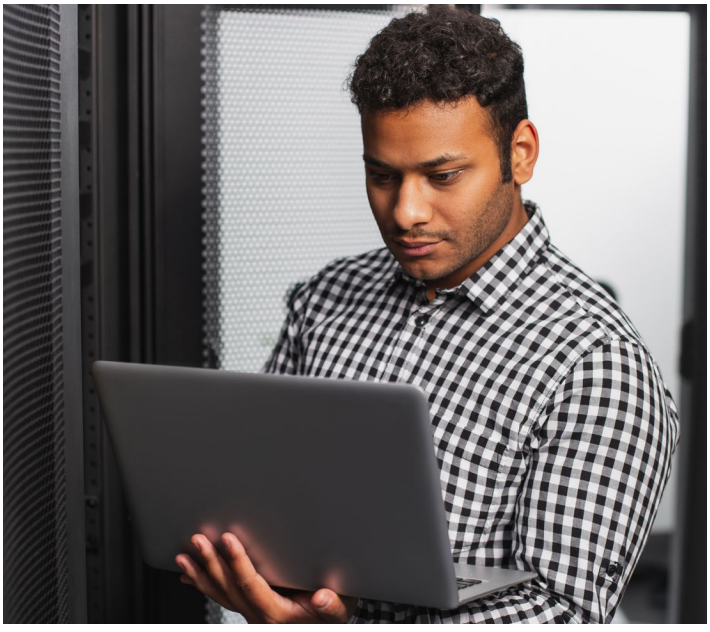
Brown & Brown INSURANCE®

COVID-19: CYBER SECURITY AND REMOTE WORKFORCES CONSIDERATIONS

As more and more social distancing measures are enacted, employers are transitioning their workforce to remote workstations en masse. The COVID-19 outbreak is presenting a myriad of challenges, but for IT teams, specifically, equipping employees with the necessary tools and systems to maintain their productivity is uncharted territory.

In this unprecedented time, maintaining security is of the utmost importance. We've already seen evidence that cyberattacks could become more focused as government agencies and companies move swiftly to adapt to COVID-19. One recent example includes the attack targeted at the U.S. Health and Human Services Department (HHS) on March 16. In that instance, the attack overloaded the HHS servers with millions of hits over several hours; however, the attack did not significantly slow the agency's systems. HHS anticipated increased attacks and added extra protections in place.

To help ensure that your organization's response to cyber threat is more akin to that of the HHS, our subject matter experts give guidance on mitigating your risk.



Stress on IT Resources

Increased remote workers inevitably bring an immediate surge of requests on the IT team. These are the first steps in implementing or rolling out remote viabilities to your teams.

- Practice a dry run for anyone who may need to work from home. This can be done in waves to maintain business continuity and availability.
- Roll out capabilities as they are available. Your teams may have limited remote capabilities at the moment, but continue to distribute tools and resources as they become available.
- Expect increased expenses as more technology, computers, access or subscriptions are needed to keep your workforce productive and secure. Proactively work with finance to define the scope of expansible items.
- Implement a Virtual Private Network (VPN) and multi-factor authentication and any other layers of protection needed for your line of business. Using a remote desktop without a VPN may leave your network exposed to hackers and ransomware attacks.

Remind Employees of Online Best Practices

Companies are always vulnerable to cyber and phishing attacks, but an increase in remote workers may present new dangers. As everyone checks their hand-washing routine, it is important to remind employees of best practices for online security.

- Be wary of suspicious links, especially those about COVID-19, including cure claims, donation requests and links or documents from unfamiliar email addresses.
- Ensure home Wi-Fi has a strong password. Instruct

employees on minimum lengths or complexities of passwords and resources on how to update their passwords.

- Update or increase security requirements on work passwords. With increased potential exposures, consider increasing the complexity and frequency of password resets.
- Explain any policies about using public Wi-Fi and the risks of using it.
- Clarify acceptable options for working and which platforms cannot be used. For example, explicitly say if employees can or cannot use platforms like Zoom, Slack, Google Drive, Google Hangouts or other shared platforms.
- Direct employees on at-home printing protocols and if and how they can print sensitive materials and how to dispose of them appropriately.

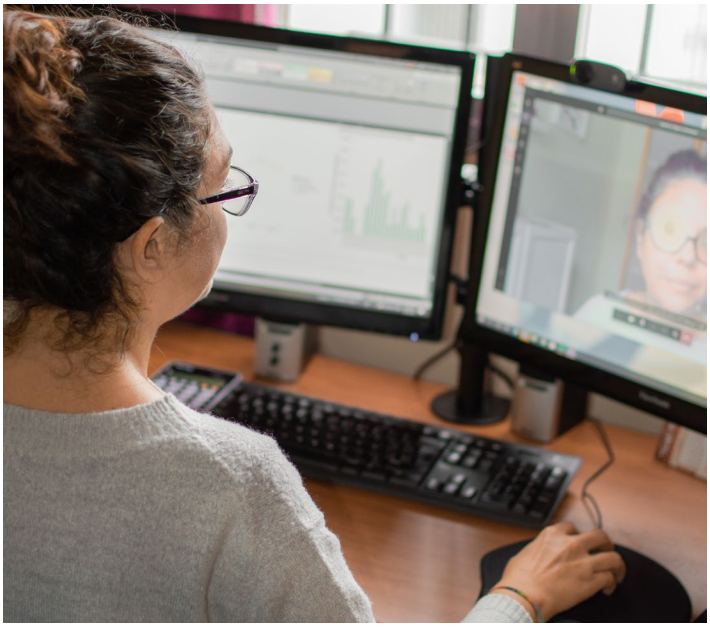
Increase in Scams

Experts expect to see an increase in scams targeted to personal and company emails. Current circulating malware, virus and phishing scams include:

- Links to COVID-19 maps that are on websites loaded with malware.
- An email saying that a person at an event you attended may have COVID-19. The email includes a link to stay updated on the status of the individual's diagnosis; however, the link is malicious.
- Luring people to download documents that appear to be from an official health authority but really contain malware or other harmful code.
- Emails containing a link to learn about a new COVID-19 cure.
- Spoofed emails from CDC or WHO claiming to have updated information on the virus.
- Donation requests for fraudulent charities or groups posing as COVID-19 causes.
- Promoting fake cures or protections.

For Small Businesses Struggling with Remote Capabilities

Technology companies are easing the transition cost to try remote tools. These tools can ease the transition process for small or large businesses not equipped to work entirely remotely. Instruct employees on any



restrictions surrounding these platforms to ensure that all sensitive or secure items are kept that way.

- Microsoft is offering a free six-month trial of its premium plan for Teams chat app (https://www.pcworld.com/article/3530374/microsofts-solution-for-covid-19-is-a-free-teams-subscription-for-six-months.html)
- Google is giving free access to its enterprise version of Hangouts Meet to all G Suite and G Suite for Education users now through July 1, 2020 (https://cloud.google.com/blog/products/g-suite/helping-businesses-and-schools-stay-connected-in-response-to-coronavirus)
- LogMeIn is offering free "Emergency Remote Work Kits" for three months (https://blog.gotomeeting.com/coronavirus-disruptions-and-support/)
- Cisco Webex expanded free Webex to all countries where it is available, is providing free 90-day licenses to non-Webex customers and is allowing existing customers to expand their usage at no additional cost (https://blog.webex.com/video-conferencing/cisco-webex-supporting-customers-during-this-unprecedented-time/)

Know Your Coverage

If you have any questions or concerns about your cybersecurity insurance coverage, talk to your account representative. We will continue monitoring the situation and share new information as it becomes available.

Sources:

https://www.marketwatch.com/story/working-from-home-because-of-coronavirus-dont-give-your-company-a-different-kind-of-virus-2020-03-11
https://www.theatlantic.com/ideas/archive/2020/03/coronavirus-creating-huge-stressful-experiment-working-home/607945/
https://www.bbc.com/news/technology-51838468
https://www.washingtonpost.com/technology/2020/03/12/hackers-are-using-coronavirus-fears-target-people-looking-information-infection-maps/
https://www.scmagazine.com/home/security-news/news-archive/coronavirus/coronavirus-tracking-app-locks-up-android-phones-for-ransom/
https://www.scmagazine.com/home/security-news/news-archive/coronavirus/russian-cybercrime-forums-seen-selling-malware-sabotaged-covid-19-map/
https://www.benefitspro.com/2020/03/16/cyberattack-hits-hhs-amid-covid-19-outbreak/