Cybersecurity Tips to Prevent Your Business from Becoming COVID-19's Virtual Victim

troutman sanders

While protecting the health of employees and clients should be every organization's top priority, businesses would be naïve to ignore the cyber risks presented by coronavirus (COVID-19), which has forced a majority of businesses to shift to remote work. Hackers, looking to capitalize on fragmented operations and inherent employee vulnerabilities that exist even in absence of crisis and panic, are leveraging COVID-19 to carry out attacks. We have already seen a COVID-19 spear phishing attack used to infect computers with a remote access Trojan, and a malicious COVID-19 Android App that installs ransomware on the affected phone. Whether it be through phishing, credential theft, or by malicious links shared through social media, not even cybersecurity is immune to this virus. If you had a business interruption plan that included a contingency for pandemic, deploy it and review the below to make sure it is complete. Otherwise, here are a few basic precautions every business should take to mitigate the chances of becoming a virtual COVID-19 victim.

1. Raise Employee Awareness

Businesses should remind employees to be extra vigilant during this time and train them to recognize common scams and threats. We have already seen an increase in phishing scams as attackers exploit COVID-19 fears and companies deploy a remote workforce (e.g., not being in physical proximity). If an employee suspects they are being phished, encourage them to call the sender directly to verify authenticity (social distancing does not mean no contact). Consider rolling out a training program addressing specific work-from-home risks. Just like it only takes one person to spread the virus, it only takes one click to let attackers in.

2. Secure Your Remote Work Environment

With employees tasked to work remotely, review your virtual or remote work policies. Businesses should issue company devices where possible; avoid personal devices even if using a sandbox (e.g., Citrix); and remind employees that physical security controls apply at home. Indeed, a "clean house" takes on a whole new meaning. Businesses should also consider additional audits and reviews of logs to determine when sandbox controls are being avoided or broken. Once things return to normal, have a process to reel uses back in and test boxes upon return.

3. Consider Vendors with Access to Protected Information and Systems

Realize that most vendors are likely going remote and consider what that means for your organization. For example, will vendors have access to protected systems and information from their new working environment? Do your vendor contracts allow for such remote work and include necessary safeguards? Are there any precautions you should take to mitigate the cyber risks brought by vendors' remote access to protected information and critical systems? If you are a vendor, are you permitted to allow your employees to work from home? (see Secure Your Remote Work Environment)

4. Update Incident Response Plans

Remind employees how to report actual or suspected security incidents. Ensure contact information is updated for the virtual workplace – both to report an incident and to contact Cyber Incident Response Team (CIRT) members – and specify backup contacts in the event a CIRT member is ill. Additionally, ensure your CIRT and backup contacts are familiar with their roles and responsibilities and apprise them of the increased cyber risks that remote work introduces.

5. Review Cybersecurity Insurance Policies

Review your cyber-insurance policies to determine what is covered and when/how you should engage your carrier in the event of a suspected incident. Businesses should also think about how the use of personal and/or temporary storage devices used during this time may implicate policy terms. Policies should be broad enough to cover incidents that may occur while employees are working from home.