Coronavirus: Cybersecurity considerations for your newly remote workforce (United States)

COVID-19 Alert

31 March 2020

By: Jim Halpert | Steve Klementowski | Edward J. McAndrew | Rob Otten

In response to the coronavirus disease 2019 (COVID-19) pandemic, organizations around the world have moved to remote work platforms in a span of a few short weeks. Remote work programs that normally would be designed, tested and implemented incrementally over an extended period are being operationalized for entire workforces of many companies with no period of planning or adjustment. This may be the fastest and most disruptive technological shift in global work conditions in history.

Working remotely, or "teleworking," presents unique cybersecurity challenges to the employer, the employee and the supply chain, especially when being done for the first time in a rapidly changing environment. In the context of this global crisis, cyber risk management involves balancing the productivity of a workforce with ensuring confidentiality, integrity and availability of the company's own systems and data, as well as that of their supply chain.

In recent weeks, the Department of Justice, Federal Bureau of Investigation and the Department of Homeland Security have issued alerts warning of malicious cyber activity related to COVID-19. Just yesterday, the FBI issued a new Private Industry Notification entitled, "Cyber Criminals Take Advantage of COVID-19 Virus for Cyber Criminal Schemes." The Bureau writes that cyber threat actors are seeking "to profit from a sudden growth in teleworking, increased use of virtual

education systems for online classes, a surge in online shopping, public appetite for information related to the pandemic, and the criticality of maintaining functioning critical infrastructure networks."

We highlight below some of the key issues to consider as we move through this transformative period of remote working. We include some of the cybersecurity practices that are included in industry standards and legal frameworks, and that have been reaffirmed through our collective experience in cyber incident response. It is important to note, though, that cybersecurity regulation is generally sector-specific. Whether any particular cybersecurity practice is legally required is beyond the scope of this Alert. The views expressed below do not constitute legal advice.

Awareness and Training

Various laws and best practices speak of the need to train network users on the latest security best practices. Security policies and procedures may be updated to include additional guidance for working remotely and distributed to all remote employees. Employers' checklists of cyber best practices and periodic cybersecurity updates to employees generally advise them of emerging threats and remind them of related best practices. COVID-19 resource pages may also include cybersecurity information. If personal devices are used to access company resources, employers may remind employees to: (1) update their device's operating system and apps; (2) ensure anti-virus software is installed and running on all devices used for remote work; and (3) enable security features for browsers and cloud-based applications and accounts. Employees should also be reminded of best practices when connecting to Wi-Fi networks outside of their office, including securing wireless routers at home.

Email protection

Employees not accustomed to working remotely are especially vulnerable to email-facilitated cybercrime. The most prevalent schemes include phishing designed to trick them into disclosing credentials or other confidential information, as well as business email compromises focused on diverting electronic payments to criminals' accounts. Sophisticated attacks can tailor messages individually to dupe specific employees. Governments and cybersecurity experts are reporting a surge in COVID-19-related phishing activity.

Employees should be on alert for increased phishing attempts related to the current situation. Where appropriate, employers may consider providing specific examples to illustrate how to spot malicious messages or engaging a security firm to send test phishing messages. Employees may be reminded to use government or trusted news sources for information about COVID-19 and to verify the URL for such sites before interacting with them. Enabling "safe searching" browser security features can help. As part of an organization's continued cybersecurity messaging, employers also should strongly consider reminding employees to be vigilant and not to disclose credentials or personal or business confidential information over email or to any untrusted website to which they are directed by email.

Among the ways to potentially combat phishing attempts: (1) double checking the email address of the sender; (2) confirming that the email address is the same and is correct on a reply message; (3) paying close attention to grammar/typos, wording, sentence structure, tone and context for any message seeking information or some responsive action; and (4) using a separate form of authentication (usually and most easily phone calls to a "known good" number) to confirm the authenticity of the email communication and any request for a funds transfer above a de minimis amount. Where feasible, consider using encryption and secure file transfer platforms for the transmission of sensitive data.

Secure systems enabling remote access

Virtual Private Networks (VPNs) are a common tool used to enable secure, remote access to an organization's internal networks. It is a best practice to use VPNs or other secure "tunnels" whenever feasible, particularly if users are working from personal devices. Businesses should strongly consider confirming that systems enabling remote access, such as VPNs and other network infrastructure devices, are patched to the highest available version. Systems not previously made available outside of a business's network may now be exposed out of necessity. Best practices generally include having IT administrators validate system configurations against security standard and reference architectures for those systems. Industry standards and various laws require different systems on the enterprise network to be limited to those with a business need and on a "least privilege" basis. Security departments are also encouraged to consider adjusting security monitoring alerts to reduce false positives and provide additional oversight given the atypical usage patterns caused by heavy telework.

Multi-Factor Authentication

Multi-Factor Authentication (MFA) is a powerful tool in combating potential unauthorized access to systems where access credentials have been lost or stolen. As additional systems are made accessible outside of the business's network and employees are targeted in phishing attempts, this additional layer of security can potentially help prevent many intrusions. Where feasible, it is a best practice for employees with remote access to have MFA enabled on their accounts. Some newer laws, such as the New York Department of Financial Services Cybersecurity Regulation, require MFA under certain circumstances. If hardware-based tokens are not available on short notice, many MFA providers support software-based tokens that can be rolled out easily and quickly. Where organizations must allow employees to use personal or commercially available accounts for work purposes, consider whether MFA controls may be utilized where available.

Non-standard cloud technology

Employers should reaffirm which hardware, software and tools are approved and available for their remote use and how confidential information should be handled. These controls work best where employees are made aware of which tools may be used to store and share files securely while working remotely. Blacklisting certain email and file-sharing websites and setting up a process for exceptions can effectuate policies that limit the use of non-standard technology.

Business continuity and IT support

IT practitioners have been working tirelessly to set up and support their user populations with secure, remote access. As employees work from home, organizations can expect an onslaught of IT issues related to remote access. Help desks may be overburdened and face significant delays triaging and identifying critical issues. IT managers are strongly encouraged to consider holding regular touchpoints with business leaders to identify critical issues affecting the remote workforce and align on priorities for resolution. Asset criticality ratings may be revisited and adjusted to ensure adequate attention is given to resources that are critical to the remote workforce.

In light of the heavy demands on IT support currently, consider setting up alternative, out-of-band channels for reporting potential cybersecurity incidents. Lastly, employers are strongly encouraged to consider reminding employees of their responsibilities related to reporting potential incidents.

Time to revisit your cyber incident response plan

Every organization is encouraged to review – and revise, where necessary – its cyber incident response plan to account for new attack risks to its own network, as well as on its supply chain. Incident responders need out-of-network access to scenario-specific response protocols, business continuity/disaster recovery plans, team contact lists, key vendor agreements, communications packets, law enforcement contacts and legal resources (contract matrixes, data breach notification requirements, etc.). It is always best for alternative, out-of-band communications channels to be established for the incident response team and key incident response stakeholders. Businesses are urged to analyze cyber insurance policies for notification obligations and required approvals for the use of response vendors (legal, forensics, public relations, notifications, etc.). If they are not already in place, employers may also seek to negotiate and execute master service agreements with external response vendors – in advance and under legal privilege – to ensure that scalable resources are at the ready if needed. A best practice is to prepare a litigation preparedness plan to ensure that any incident response is executed in a manner that mitigates potential liability and litigation risk. Lastly, employees should be reminded of their responsibilities related to reporting potential incidents, including the channels for doing so while working remotely.

The path forward

As the situation continues to change rapidly on both global and national scales, it is imperative that we remain attentive to government guidelines, directives, laws and orders (whether issued by the CDC or other federal, state or local health authorities).

This alert highlights only some of the key issues raised by this rapid transition to remote work. It is not intended to be comprehensive, and it does not constitute legal advice.

Please contact the authors, any member of the DLA Piper Cybersecurity Team, or your DLA Piper relationship attorney if you would like more specific advice, whether on cybersecurity matters or any wider business issues.

And please visit our Coronavirus Resource Center and subscribe to our mailing list to receive alerts, webinar invitations and other publications to help you navigate this challenging time.

AUTHORS

Jim Halpert
Partner
Washington, DC | T: +1 202 799 4000
jim.halpert@dlapiper.com

Edward J. McAndrew
Partner
Wilmington | T: +1 302 468 5700
Washington, DC | T: +1 202 799 4000
ed.mcandrew@dlapiper.com