If you cannot view this email correctly, please view it online.

Forward to a Colleague

ALERT

MARCH 2020

Coronavirus and Remote Work Heighten Cybersecurity Risks

As increasing numbers of employees work remotely in response to the novel coronavirus (COVID-19) outbreak, companies should be mindful of increased data security risks and take prompt, practical steps to mitigate them.

Increased Risks

The sudden and dramatic surge in the use of telework presents heightened cyber risks, including:

- An increased incidence of phishing attacks using coronavirus references as bait to induce employees to click on email links or attachments infected with malware.
- Enhanced risk of cyberattacks on company networks due to reduced IT staffing and/or need to focus on supporting remote access at the expense of security.
- Business continuity risks arising from the potential lack of system and connectivity resources to handle surge in remote work, compounded by the heightened risk of cyberattacks that could disrupt operations.

Recommendations

These risks have prompted the federal government's Cybersecurity and Infrastructure Security Agency to urge companies to adopt a heightened state of cybersecurity. Companies should take the following steps to mitigate the increased risk:

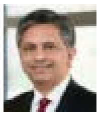
- Issue Employee Communications
    - Alert employees to expect increase in phishing attempts, especially coronavirus-related emails.
    - Prompt employees to use strong passwords, especially if multifactor authentication is not implemented for remote network access.
    - Remind employees of company's information security policies governing remote work and use of personal devices or, if no formal policy exists, issue guidelines promptly, instructing employees:
        - Not to download company information onto personal devices or email accounts or unauthorized cloud or other third-party services;
        - Not to use public or insecure home networks, at least without a virtual private network ("VPN") connection;

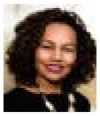
        - To protect against unauthorized third parties accessing any company data; and
        - To protect the physical security of the company's devices.
- Prioritize Information Security
    - Update security configurations and access controls and patch VPNs and other network infrastructure.
    - Dedicate resources for targeted monitoring and detection of cyberattacks (including review of logs that might reveal anomalous activity from outside connections).
- Incident Response Plan
    - Update contact information for incident response team, establish secure communications channels, and confirm incident reporting protocols for employees working remotely.

SHARE THIS ON LINKEDIN

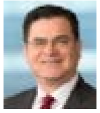
FORWARD TO A COLLEAGUE

Lisa M. Ropple
Boston


Samir C. Jain
Washington

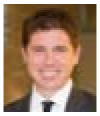

Jennifer C. Everett
Washington

Daniel J. McLoon
Los Angeles


Mauricio F. Paez
New York

Todd S. McClelland
Atlanta

Richard J. Johnson
Dallas


Aaron D. Charfoos
Chicago

SUBSCRIBE   SUBSCRIBE TO RSS

Jones Day is a global law firm with more than 2,500 lawyers on five continents. One Firm Worldwide®

Disclaimer: Jones Day's publications should not be construed as legal advice on any specific facts or circumstances. The contents are intended for general information purposes only and may not be quoted or referred to in any other publication or proceeding without the prior written consent of the Firm, to be given or withheld at our discretion. To request reprint permission for any of our publications, please use our "Contact Us" form, which can be found on our website at www.jonesday.com. The mailing of this publication is not intended to create, and receipt of it does not constitute, an attorney-client relationship. The views set forth herein are the personal views of the authors and do not necessarily reflect those of the Firm.

North Point, 901 Lakeside Avenue, Cleveland, Ohio 44114-1190
www.jonesday.com

Click here to opt-out of this communication.
Click here to update your mailing preferences.
Click here to view our privacy policy.