JANUS Coronavirus COVID-19 Update #6 – March 18, 2020

COVID-19 is continuing to rapidly spread throughout the U.S. Businesses are struggling to provide the necessity of allowing workers to remotely access company networks, but a major issue is if your organization is prepared for the increase in traffic, as well as the ramifications to your enterprise and business operations.

JANUS, the nation's oldest cyber security, privacy and business continuity consultancy is fully operational in these troubled times, and we would like to continue to share useful information that could make the transition to work remotely easier, more efficient, and also safer from a security standpoint. Below are suggestions and links to information on how best to prepare and protect yourself and your operations as you move to a remote workforce. We hope you find this information in the areas of IT Cyber Operations, Personnel, and General Information useful. We urge you to forward this email to anyone you feel may benefit from its content.

IT & Cyber Preparations

1. **2-Factor Authentication:** If you are using 2-factor authentication, is it functioning correctly? Do your employees know how to use it? Don't take for granted that they remember how it works.
2. **Support/Help Desk Staffing:** Have you considered how workloads may increase if remote access spikes? Are there enough personnel available to cover the increased workload? Is the team well versed on remote access procedures?
3. **Remote File Access:** It is mission critical that remote employees have access only to the files and servers necessary for them to perform their jobs. Now is a good time to review file access permissions and confirm that employees have appropriate access to files and servers. Data spills (breaches) often occur due to inappropriate file access by current employees.
4. **Increased Virus & Malware Risks:** If the employee is using his/her own computer at home, remote access has the increased potential of a virus, malware, or ransomware getting into your network via a Virtual Private Network (VPN). Remember, you have no idea where your personnel have surfed on their personal machine, what level of protective software they have installed, and whether it's up to date. You also have no idea if they are current on critical operating system patches. Consider offering them access to a company funded endpoint security package. While this may seem costly at the onset, the financial and operational ramifications will be substantial should they accidentally drop ransomware on the corporate network.
5. **Firewall, Endpoint Protection:** Now is a good time to confirm that all of these items are properly configured. Make sure that the necessary functions in each of these is configured appropriately and that all generic login and password credentials have been deleted or deactivated.
6. **Log Monitoring:** Ensure that an audit trail for all actions on the VPN/web platform is maintained including, but not limited to:
    1. Logins
    2. Failed login attempts
    3. Impossible IP address logins
    4. User activity while active
    5. Upload/download activity
7. **Data Loss Prevention (DLP):** With the marked increase of remote access, consider regular scanning of data flows for any leakage.
8. **Patches:** Confirm that all patches have been applied. If they aren't, consider first addressing the most critical, followed by less critical. Getting your patch work done has never been more important as hackers are already using this situation to their advantage.
9. **Additional Remote Equipment:** In circumstances where key employees will be working for an extended period of time with a company laptop, consider offering them a kit to take home. This kit could include a monitor, keyboard, mouse and power supply. Offering them these items will allow them to work more efficiently and maintain a higher level of productivity in both the short and long term.

Personnel Related

1. Comprehensive FAQs For Employers On The COVID-19 Coronavirus from the law firm, Fisher Phillips
2. Privacy Considerations for Employers and Health Care Providers When Communicating about Coronavirus-Infected Individuals from the law firm, Proskauer Rose LLP
3. BULLETIN: HIPAA Privacy and Novel Coronavirus: Office for Civil Rights, U.S. Department of Health and Human Services

Web Sites

The Internet is rife with misinformation on everything including COVID-19. It is important that you obtain your information from reliable sources. Below are links on a wide variety of topics from reliable sources and subject matter experts.

1. The U.S. Centers for Disease Control (CDC): https://www.cdc.gov/coronavirus/2019-ncov/index.html
2. The World Health Organization (WHO): https://www.who.int/emergencies/diseases/novel-coronavirus-2019
3. The Association for Bio Safety & Bio Security: https://absa.org/coronavirus/
4. National Association of State Legislators COVID-19 Resources for State Legislators and Staff: Click here
5. Infectious Disease Society of America COVID-19: Resource Center: Click here
6. EDUCAUSE Higher Education COVID-19 Resource Page: Click here
7. SBA Guidance for Businesses and Employers to Plan and Respond to COVID-19: Click here
8. US Department of Labor COVID-19 Resource Page: Click here:
9. Information for Health Professionals - Waiver or Modification of Requirements Under Section 1135 of the Social Security Act: Click here
10. HIPAA and COVID-19, view the HHS Office for Civil Rights' (OCR) March 16, 2020, Bulletin on the HIPAA Waiver: Click here
11. HIPAA Disclosures for Emergency Preparedness Decision Tool: Click here
12. Coronavirus and Employers: Critical Compliance Information from the law firm of McBrayer McGinnis Leslie & Kirkland PLLC: Click here

In closing, we all hope that this event will not be as severe as it appears to be shaping up to be. Panic and knee-jerk reactions are always ill-advised. Thoughtful what-if planning should rule your processes moving forward, and knowing that you have a well thought out plan of action to deal with any scenario will allow you and your organization to minimize any down-side risks and disruption to your business. The team at JANUS is fully operational and stands ready to answer any questions you may have and assist you in your continuity planning and secure connectivity. Please feel free to contact us at any time.

Lyle A. Liberman
Chief Operating Officer
JANUS Associates, Inc.
1.203.251.0200 (w)
http://www.janusassociates.com