## JANUS Coronavirus COVID-19 Update – February 27, 2020

The World Health Organization has told countries to prepare for a coronavirus pandemic, and the U.S. Centers for Disease Control (CDC) has said it expects a sustained transmission of the coronavirus (COVID-19) virus, and has called for businesses, schools, and communities to brace themselves and plan for potential outbreaks and disruptions.

The question to ask yourself is are you prepared for a possible pandemic and its ramifications to your enterprise and business operations? JANUS is the nation's oldest cyber security, privacy and business continuity consultancy and we would like to share some suggestions with you on how best to prepare and protect yourself and your operations should a worst case scenario play out. We hope you find these suggestions useful in your preparations, and we urge you to forward this email to anyone you feel may benefit from its content.

**Personnel Related**

1. **Hand Washing:** Wash your hands often. This tried and true method is effective at limiting the spread of all pathogens, not just COVID-19.
2. **Disinfection Products:** Products such as Lysol and bleach have not been proven to kill or limit the spread of COVID-19. There is nothing wrong with using these products to disinfect surfaces, but don't be lulled into a false sense of security. While labels may say they kill Coronavirus, they are referring to strains such as MRSA and currently, the EPA has not set testing guidelines for products that will kill COVID-19.
3. **Workplace Disinfection:** The length (time) of surface persistence of COVID-19 is uncertain at this time according to the CDC so cleaning with disinfectants may help but the EPA recognizes that in the event of an emerging viral pathogen, the strain is likely not available for testing and that existing disinfectants will not have the specific virus on the label.
4. **Masks:** The Centers for Disease Control and Prevention says it "does not recommend that people who are well wear a facemask to protect themselves from respiratory diseases, including COVID-19." "Facemasks should be used by people who show symptoms of COVID-19 to help prevent the spread of the disease to others," the CDC's website says. "The use of facemasks is also crucial for health workers and people who are taking care of someone in close settings (at home or in a health care facility)." If you choose to use a mask, make sure the type is an N95 FFR as this type is designed to filter out particles as small as 3 micron, including viruses.
5. **Symptomatic Employees:** Have or prepare a written action plan to follow in the event that an employee starts showing signs of infection. Consider reviewing this plan with managers so they understand what to do should a team member fall ill during the work day.
6. **Confirmed Employee Illness:** Review or prepare a written policy regarding an employee who has tested positive for COVID-19 in regards to time away due to illness, and what medical clearance will be required in order to return to work. Consider sharing this information with all employees as soon as practical in order to allay any concerns when a colleague returns to work.

**Business Operations Related**

1. **Business Continuity Plan:** If you have a Business Continuity Plan, now is the time to review and update it if necessary. Pay attention to how old it is. There can be lots of changes to your operations in a short period of time and even things like minor personnel changes or a new software application can have a profound effect on the performance of the plan.
2. **Facilities Preparation:** Do you have appropriate facilities for key personnel should travel be restricted? This includes sleeping, toilet, and eating areas, adequate supplies of food, and sufficient supplies and equipment for cleaning and maintenance personnel.
3. **Restricted Travel:** A worst case scenario might prevent employees from traveling to work due to employee fear or government mandate. Now is a good time to review all roles and responsibilities to ensure that other team members have the capability to perform a task should the primary employee be absent. It's wise to speak with the alternate team members to confirm their understanding of the task should they be called on.

4. **Employee Communication:** You may need to contact a team member during off-hours. Now is a good time to review and update all contact information including current addresses, phone numbers and personal email addresses.

## IT & Cyber Preparations

1. **Remote Access:** If necessary and allowed, are your employees prepared to log in remotely? When was the last time they tested their VPN connections? Consider issuing a "How To" document to all employees who will be granted remote access. Doing so will cut down on Help Desk requests.
2. **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.
3. **Support/Help Desk Staffing:** Have you considered how their workload 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?
4. **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.
5. **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 the 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.
6. **Firewall, Endpoint Protection, DLP, Log Monitoring:** Simply stated; 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 are appropriately set and that all generic login and password credentials have been deleted or deactivated.
7. **Patches:** Now is the time for you and your team to confirm that patches are up to date. If they aren't, consider first addressing the most critical, followed by less critical. Getting your patch work done has never been more important.
8. **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.

## Web Sites

The internet is rife with misinformation on everything including COVID-19. It is important that you get your information from reliable sources, not a conspiracy site, or Facebook. Below are 3 links that should serve you well.

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/

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 stands ready to answer any questions you may have and assist you in your continuity planning. Please feel free to contact us at any time.

Gary Fielding
Director
JANUS Associates, Inc.
1.203.251.0200 (w)
http://www.janusassociates.com