FORTALICE CLIENT ADVISORY

Coronavirus Cyber Advisory

06 March 2020

Fortalice

Executive Summary

Recap of Current Events

At Fortalice, the security and resiliency of your company matters greatly to us. This advisory was written in accordance with our desire to keep our clients informed.

Based on the latest World Health Advisory (WHO) Advisory, we have a few recommendations we believe will be useful to you. Our hope is that this advisory equips you to take the necessary preemptive steps to protect and defend your company from any potential issues from the Coronavirus outbreak.

The loss of life due to illness is tragic. In addition to the impact that the cold and flu season has on the workplace, COVID-19 is a relative unknown and is striking fear and concern around the globe. The long-term impacts on supply chain are not truly known and this can impact the operations of your organization.

In light of these events, Fortalice is urging our clients to review and practice the elements of their Business Continuity Plan and Resiliency Plan (BCP/RP).

Fortalice

RECAP OF CURRENT EVENTS

The Fortalice team also regularly tracks global issues, analyzing their impact on the way Nation States and cybercriminals conduct their affairs. Regarding Nation States and cybercriminals and their cyber capabilities, we are providing guidance to secure your operations regardless of whether or not you need employees to operate on premise or remotely.

Manipulation and Social Engineering Campaigns

- The WHO, FBI, U.S. Department of Homeland Security (DHS), and firms like ours are finding that cybercriminals and Nation States are leveraging the crisis to socially engineer your employees. The scams and lures are posted on social media and are delivered to both personal and professional email accounts.
- In the latest scams, they may pose as the health care provider or a supplier of workplace hand sanitizer. Often, they will use sensational, and at times false or misleading, news stories on social media to bolster their scam. There is a danger that an employee takes the bait and is tricked into sharing inside company information and personal information, such as how many employees are sick, if people are working remotely, and other clues that can assist the digital attacks they are planning.
- Motives of the attackers vary, some motives include: (1) Create fear and panic; (2) Conduct Business email compromise and wire transfer scams with employees working remotely; and (3) Employ social engineering campaigns to gain access to company files and information.

While our international clients enacted their BCP/RP weeks ago, there are additional steps all organizations should take whether you have enacted your BCP/RP, or are on watch-and-warning to do so. We recommend that all of our clients consider taking the following steps during the crisis. For those clients in geographies that have not been hit as hard, this is the perfect time to refine your plans and approach. For context, consider what your company would do if you find yourself in a similar situation to these following real-life scenarios. On 05 March, for example, banking giant, HSBC, was forced to evacuate a floor from its global headquarters in London after a worker tested positive for coronavirus. On the same day, Microsoft announced that employees in their Washington State facility will work remotely. **If you were told you needed to send a whole division of workers home, the questions to consider and the recommendations below are designed to ensure you do not negatively impact your operational security and resiliency.**

5 QUESTIONS LEADERS SHOULD ASK

1. Is our BCP/RP current and has it been tested within the last 12 months? What is our work-from-home policy? Is our remote work plan easy to follow and secure?
2. Do our 3rd party vendors have a BCP/RP?
3. Will customer facing processes work well if all of our employees are remote and if we are dealing with a limited workforce due to illness?
4. Will our internal processes (e.g., payroll, accounting, invoicing, HR) run with staff working remotely? If yes, how?
5. Are our remote work processes securing our digital assets and our customers' privacy?

Gartner did a poll of companies to ask the biggest barriers to pandemic planning and 54% of HR leaders stated that "poor technology and/or infrastructure for remote working is the biggest barrier to effective remote working."

Source: https://www.gartner.com/smarterwithgartner/with-coronavirus-in-mind-are-you-ready-for-remote-work/

STEPS TO TAKE THIS WEEK/MONTH

1. Immediate Housekeeping Items

- Update remote software such as your Virtual Private Network (VPN).
- Call your VPN provider to ask them if they can handle the load of all staff working from home and adjust accordingly.
- Fine tune your email filtering strategies and double check your SPF header records and DMARC.
- Update all operating systems, browsers, office productivity software and antivirus.
- Send out employee education and awareness reminders.

2. Contact Vendors

- Call your vendors to ask them how prepared they are to withstand a pandemic. Make sure you have a playbook in place detailing what you will do and how they will support you.
- Contact your local suppliers of phone and internet to ensure they can handle the load for one or more employers to send their employees to work from home. Plan accordingly to provide critical functions with cellular mobile hotspots.

3. Practice the Pandemic Situation

- Choose a day in the next two weeks and practice the entire work-day with all employees working remotely for the full day.
- Plan to practice your incident response playbook and pay special attention to figuring out how you would respond to different issues, how escalation will work, and what your communications plan will be for your employees and customers.

4. Fine Tune Protection Strategies - #1 Avoid Dangerous Emails

- Train employees that all "news" on social media sites and sent via emails could be a trap. Encourage staff to use VirusTotal before clicking on a link or opening an attachment, even for internal emails! VirusTotal will scan more than 50 sources and notify you if a link or file is bad: www.virustotal.com.
- Avoid Business Email Compromise (BEC): Implement new wire transfer protocols to institute steps that an attacker could not guess that you would take. Example: send a secret pre planned GIF back and forth that an attacker would not guess as a way to let the person receiving the message knows it is really you.

5. Add a Deadbolt to the Cyber Door with Updates / Anti-Virus / Multifactor Authentication

- Accelerate plans to institute Multi-Factor Authentication (MFA) on key systems
- Review FBI InfraGard and DHS CISA bulletins for ongoing information around indicators of compromise.
- Ask your security team or provider for the latest blocks to add to block known bad web links and internet protocol addresses.

6. Create A "Shields Up" Approach Through A Segmentation Strategy and Kill Switches

- Segment data, user access, and networks.
- Start small by setting up more than one domain name to segment your core public facing operations from your back office.

7. Enhance Your Remote Strategy

- Publish your company approved web and cloud tools and processes for remote work.
- Train your employees on best practices via an all-hands conference call.

8. Stay Informed

- Fortalice will post information updates to our social media accounts as we see them.

Educational Resources

Be sure to keep the lines of communication open with your employees. Please consider sharing the following links with your staff:

- World Health Organization (WHO) – Q&A on coronaviruses (COVID-19) https://lnkd.in/eq2kRdS
- Overseas Security Advisory Council (OSAC) – COVID-19 (Coronavirus) Outbreak Resources https://lnkd.in/ekcFGWP
- U.S. Centers for Disease Control and Prevention (CDC) – Coronavirus Disease 2019 (COVID-19) https://lnkd.in/eKC_t4c
- FBI Updates https://www.infragardnational.org/resources/coronavirus-disease-2019-covid-19-resources/
- DHS CISA Updates https://www.cisa.gov/coronavirus
- Fortalice Fix for Business Email Compromise (email Watchmen@FortaliceSolutions.com to request)

CONTACT FORTALICE

Contact Fortalice

Need help refining your BCP/RP? Need help locking down the security of your remote workforce through tools, apps, fine tuning security solutions, and processes? We are here to help.

Fortalice Solutions, LLC remains the cybersecurity and intelligence operations expert companies and people turn to regarding efforts to strengthen their privacy and cybersecurity. If you would like to step up your cybersecurity defenses or need help complying with existing or future regulations, give us a call. We are highly skilled in disaster planning and recovery, incident response exercises, and cyber risk assessment, and we are standing by to aid you and your team.

Contact:
Call **877.487.8160** or email Watchmen@FortaliceSolutions.com

Note: If you'd like to see the Fortalice employee message and specific Coronavirus policy, write to Watchmen@FortaliceSolutions.com.

APPENDIX – DEEPER INTO TACTICS

Going a Little Deeper For the Practitioners

Practice the Pandemic Remote-Work Now

- Choose a day and send all employees home. Enact your phone tree and account for everyone.
- Have employees test out the quality and speed of their home services. Note the workload and stress on the remote access of the systems.
- If feasible, simulate remotely accessing systems used for critical and time sensitive transactions (e.g., trades, wires).
- Do a few scenarios where you simulate the VPN becoming overloaded or a portion of users cannot access the corporate email systems.
- Review processes (e.g., written records of phone calls) where oversight and regulatory requirements need to be enforced, even from home.
- Work with internal and external counsel to discuss the gray areas and ask regulators if there will be flexibility afforded on some rules. For example, past hurricanes and earthquakes in the United States have led to relaxed rules that favored resiliency of operations.
- Conduct a hot-wash the next day while it is still fresh, noting areas that need improvement such as:
    - Barriers to getting work done;
    - Slowness or lack of access;
    - People getting kicked off the Video conference platforms, VPN, email, other key business functions;
    - Authorizations and logins via remotely not working

Secure the Remote Worker

- Ensure you have a remote work policy and post it for employees to access. A great policy will include company do's and don'ts when accessing the corporate network.
- Do a quick security refresher training for employees. If you are not sure where to start, try some of the free resources at OnGuardOnline.gov.

Establish company tools and guidelines for:

- File sharing
- Accessing company files remotely via VPN
- Video and teleconferences
- Removable media
- Printing company data
- Working from home doing company business while significant others, roommates, and family members are present in the home

Zero-Trust

- Assume all of your employees have unsafe home equipment and their broadband internet or Wi-Fi is not secured.
- Provide guidance regarding Internet of Things devices that may be present in the room and on the home internet access points where employees work.

VPN Vulnerabilities

- VPN, virtual private networks, are not a "set it and forget it" tool.
- The US government warned last year that vulnerabilities in VPNs allowed attackers almost completely masque access to networks.
- Make sure your VPN choice is secured and patched at all times.

Managing Remote Identity & Behavior Based Analytics

- Install multi factor authentication on all accounts and access points.
- For example, access points such as payroll, company files, company email, and more should be protected behind MFA.
- Note logins and pay careful attention to out of the norm login attempts.

Behaviors to Track Could Include:

- Browser choice
- Type of device
- Login irregularities by day of week, hour of day
- Logins out of the norm for a geographic location
- Sudden use of Tor or proxy servers to connect to your VPN
- A user or device or system has unusual patterns of data movement or transfer
- Look for scanning activity