March 10, 2020

COVID-19 and Your Cyber Security

As the COVID-19 virus spreads in the US over the coming weeks, many companies and organizations will encourage or require employees to work from home (WFH, hereafter). Because you will likely move to this stage soon, we encourage you to take steps now to ensure that WFH works smoothly from an IT perspective and does not endanger your cyber security.

The right steps will vary for each company depending on a variety of circumstances: what work is critical and/or sensitive; how the organization's IT infrastructure is set up; what Bring-Your-Own-Device policy is in place; and so on.

Here are a few steps for organizations of all sizes and sectors to consider:

1. Assess criticality and sensitivity of work requirements

Business leaders should determine what work must get done during a sustained WFH and what work can be deferred or de-prioritized, as well as what work involves accessing sensitive information or systems, and what work does not. Prioritize work that must get done and involves handling sensitive information first, and de-prioritize work that does not have to get done and does not involve sensitive access.

2. Restrict personal device usage during WFH

Often, personal devices have already been infected by malware. Processing company materials on these devices or using them to access corporate systems through unsecured VPN runs a high risk of compromise. Using the criteria from #1 above, prioritize enabling secure access (points # 3 and 4) for employees who have work that involves sensitive access and that must get done, and consider restricting WFH for employees working on non-critical work. Make clear to employees what materials cannot, under any circumstance, be processed on a personal device. Listen to employees who tell you they must get work done, because employees who are not provided with secure access will often find ways to "get the job done" around the system using shadow IT, creating more risk.

3. Act now to procure or issue laptops and mobile devices

The number of personnel who need remote access for a sustained WFH scenario is often greater than what was necessary under normal circumstances, so IT/Security will need to issue equipment to more people, whether with company-issued devices or BYOD with security controls in place. Buy new devices now, since supplies may run short, or identify previously used devices your organization has in reserve and re-provision them, beginning with a full factory reset. Secure devices as usual: lock down devices so employees cannot change configuration or add apps; install appropriate security software, such as Endpoint Detection & Response (EDR) and Mobile Device Management (MDM).

4. Expand and secure remote access

Employees remotely accessing files on the organization's cloud or "on-prem" servers should do so only over VPN connections (or with zero-trust protections in place). Employees will also make use of third-party applications for video-conferencing and other remote work support. Act now to ensure you have adequate licenses for all necessary applications. Ensure that remote access via VPN and to third-party applications like webmail are protected by a Multi-Factor Authentication (MFA) log-in requirement. For VPNs, ideally configure them so they only connect once the device's security state has been scanned and validated. Review firewall configurations, Access Control Lists, and network segmentation so that devices entering the network remotely have the least

GOOD HARBOR
Cyber Security Risk Management

Richard Clarke
Chairman & CEO

Emilian Papadopoulos
President

contact@goodharbor.net | 202.212.6680 | www.goodharbor.net

privilege possible. During extended WFH, personnel may not connect their devices to the corporate network for a prolonged period of time, so have a plan for patch management and updating security software in this scenario.

5. Do a dry run

Pick one day this week and do a dry run: all employees who would work from home under an extended WFH scenario should do so. By doing a dry run, organizations can test technology systems and bandwidth as well as identify employees that need additional training to work remotely, then use time back on-site the following day to work through any challenges.

6. Establish and prepare support teams now, including MSPs and MSSPs

Remote users will have many IT and cyber security support needs, which will require an expanded IT/Security support team. Establish and train that team now, potentially drawing personnel from other administrative teams that will not be fully utilized during a prolonged WFH scenario. Recognize that IT/Security personnel may also get ill from COVID-19 or be pre-occupied caring for dependents, especially during school closures, so plan the size of the team accordingly. If you use a Managed Service Provider (MSP) and/or Managed Security Service Provider (MSSP), let them know that you are activating an expanded WFH program, and ask them how they are preparing to meet their Service Level Agreement (SLA) commitments during the COVID-19 outbreak.

7. Contact your insurance carrier/broker

Review your cyber, business continuity, and disaster recovery policies to see if there are any exceptions that take effect during pandemics, or during extended work-from-home situations, and if so contact your carrier or broker to see about mitigating those exceptions to cover pandemic/WFH scenarios.

8. Watch out for new spear phishing

Malicious actors are already sending phishing e-mails with coronavirus-related subject lines or content. Refresh your employee training on phishing and remind them that new attempts will reference either coronavirus and/or work-from-home rules.

9. "Never let a good crisis go to waste"

COVID-19 has implications for cyber security in ways that are very directly visible to employees, and people are paying attention. Use COVID-19 as an opportunity to educate employees about phishing, working remotely in a secure way, and the importance of cyber security.

Finally, if you need support from us during this stressful period, do not hesitate to reach out.

About Good Harbor

Good Harbor is a boutique cyber security advisory that advises senior corporate executives, Boards, investors, and government leaders on cyber security issues and managing cyber security risk. Good Harbor provides a range of management and Board-level cyber security advisory services including the following:

- Briefing Boards and management on the cyber security threat
- Navigating governance challenges for management and the Board
- Delivering risk management assessments, strategies, and programs
- Developing policies and technology roadmaps
- Preparing to manage cyber crises through incident response plans and crisis simulation table top exercises (TTXs)
- Helping investors and parties to M&A transactions with cyber security diligence, finding value and mitigating risk throughout the investment and M&A lifecycle

The firm is headquartered in Washington, D.C. and is led by former White House advisor Richard Clarke, who advised the last four Presidents, including as Special Advisor to the President for Cybersecurity and National Coordinator for Security and Counterterrorism. Most recently, Mr. Clarke served on President Obama's five-person Review Group on Intelligence and Communications Technologies. He is the author of *The Fifth Domain: Protecting our Country, Our Companies and Ourselves in the Age of Cyber Threats.*

Good Harbor has advised numerous Fortune 200 clients and companies around the world and across sectors including financial services, telecommunications, private equity, energy, and insurance. More information is available at http://www.goodharbor.net/.