SECURITY HEALTH CHECK:

Check the health of your cybersecurity and privacy safeguards for remote-work practices

Use this checklist to gauge the health of your cybersecurity and privacy practices and policies to adequately protect your remote workforce.

Risk management and governance

- ☐ Review the organization's IT/cybersecurity risk profile as it relates to the strategy, goals, and objectives for short-term, mid-term, and long-term plans
- ☐ Review and update your current cybersecurity policies and procedures to align with remote workplace safeguards
- ☐ Perform a security and resiliency due diligence on critical third-party vendors and offshore resources in the supply chain
- ☐ Review and evaluate IT/cybersecurity roadmap and reprioritize to reflect the current environment
- ☐ Perform an analysis of your current cybersecurity (in-house and outsourced) resources to align with your current workplace environment
- ☐ Establish a robust communication strategy that includes the process and protocols to engage with stakeholders (employees, clients, third parties, etc.)
- ☐ Ensure that the legal team has reviewed the legal and liability implications of remote work
- ☐ Review and prioritize your compliance program commitments to align with current deadlines
- ☐ Train internal IT, help desk, and remote users on evolving cybersecurity threats

Enterprise applications and infrastructure

- ☐ Perform triage to identify critical applications; do not make non-critical changes to critical applications
- ☐ Deploy automated password-reset tools and establish requirements for complex passwords
- ☐ Test VPNs and other access applications such as Citrix to ensure adequate capacity
- ☐ Update incident-response plans that factor in workforce changes like a reduced on-site IT staff
- ☐ Enhance monitoring for end-to-end early detection of anomalies and suspicious activities
- ☐ Enable encryption and spam filtering for emails
- ☐ Ensure that access control policies are in place and implemented, such as privileged access management (PAM), multi-factor, and/or challenge-response
- ☐ Establish the capability to perform patch management and maintenance remotely
- ☐ Track hardware assets and software licenses with a special focus on equipment and software that are needed for telework
- ☐ Monitor privileged access by optimizing the behavioral analytics tools for detecting suspicious activity for admins and those who handle critical data
- ☐ Ensure that firewalls are properly configured
- ☐ Install anti-malware and intrusion-prevention software on all systems
- ☐ Encrypt company-provided laptops via tools such as BitLocker

CohnReznick
ADVISORY • ASSURANCE • TAX

CohnReznick

Remote workforce

- ☐ Ensure that home routers and WAPs are password-protected and that the provider's default password has been changed
- ☐ Ensure that all mobile devices, including personal devices, that are used to access email and corporate networks are secured with passwords and anti-malware applications
- ☐ Avoid using public Wi-Fi and other unsecured networks
- ☐ Safeguard your devices; do not leave them unattended in public places
- ☐ Provide employees with a checklist to enable and empower them to be secure
- ☐ Whitelist and flag external emails. Inform employees about an expected increase in phishing attempts and ask them not to click on unknown suspicious links
- ☐ Be careful to not access/download sensitive information from/to personal laptops or devices. For any files on personal devices, check the company's policy related to file storage and backup, especially if files contain client data.
- ☐ Communicate with employees to raise awareness, enforce policies, and familiarize them with collaboration tools and new protocols

Enabling collaboration

- ☐ Evaluate collaboration tool privacy and security policies related to access, storage, and sharing of data
- ☐ Ensure adequate capacity for existing collaboration and conferencing tools
- ☐ Monitor usage of the applications and bandwidth used by such tools
- ☐ Provide adequate training in the proper and secure use of collaboration and conferencing tools
- ☐ Do not allow the use of free collaboration and teleconferencing tools
- ☐ Ensure that your virtual platform has the proper security in place

Immediate next steps:

- Perform triage to identify resources such as people, processes, and supporting technologies as they relate to changes in business operations
- Assess and monitor your remote access capabilities to ensure adequate capacity and security
- Enable or enhance collaborative capabilities
- Educate internal IT and remote workers on the changed threat landscape and communicate corporate policies on working remotely
- Start planning for a post-crisis business operating environment using lessons learned and benefits gained

Contacts

Bhavesh Vadhani, Principal
National Director, Cybersecurity, Technology Risk, and Privacy
bhavesh.vadhani@cohnreznick.com | 703.847.4418

About CohnReznick

As a leading advisory, assurance, and tax firm, CohnReznick helps forward-thinking organizations achieve their vision by optimizing performance, maximizing value, and managing risk. Clients benefit from the right team with the right capabilities; proven processes customized to their individual needs; and leaders with vital industry knowledge and relationships. Headquartered in New York, NY with offices nationwide, the firm serves organizations around the world through its global subsidiaries and membership in Nexia International. For more information, visit www.cohnreznick.com