Risk-Based COVID-19 Checklist

May 23, 2020

This checklist is intended to help employers attain agility to reconfigure strategy and process to attain value-creating and value-protecting opportunities during and after the pandemic

&

Implement their plan to prevent the spread of COVID-19 in the workplace. This is supplemental to the Guidance for Office Workspaces. This checklist is a summary and contains shorthand for some parts of the guidance; familiarize yourself with the guidance before using this checklist.

Risk and Governance

- ❏ Update and communicate acceptable use policies for employees and address the use of home computing devices.
- ❏ Identify functions requiring secure IT environments that remote working may not provide, and develop ways of performing them.
- ❏ Create cyber incident response to address current operational needs.
- ❏ Regularly communicate cybersecurity awareness messages to employees to reinforce security procedures.

IT Infrastructure

- ❏ Ensure VPN infrastructure is updated, FBI issued a advisory that Malicious cyber actors are increasingly targeting unpatched Virtual Private Network vulnerabilities.
- ❏ Provide secure access solutions with sufficient capacity
- ❏ Secure endpoints.
- ❏ Enforce software updates to remote workers.
- ❏ Reassess rules such as geo-blocking that could prevent remote access.
- ❏ Ensure help desk capability is provided as required by remote workers.

Cyber Operations

- ❏ Ensure that cybersecurity alerts and audit logs of critical systems — for example, VPNs, firewalls, endpoint security tools, and critical business applications — are centrally collected and analyzed to detect and respond to suspicious/malicious activity.
- ❏ Review/update VPN profiles and firewall rules to ensure employees are assigned appropriate privileges based on their roles.
- ❏ Enable multi-factor authentication for privileged accounts access first and then all access.
- ❏ Disable split tunneling for VPN profiles to ensure that remote employees cannot access the internet directly from their laptops while using VPNs to access corporate information systems.
- ❏ Create a reporting portal — for example, #phishing-attacks — or email address where employees can report suspicious emails.

Advice for Your Employees

Provide clear guidelines on cybersecurity for remote workers such as:

- ❏ Detecting and avoiding elevated phishing threats, including COVID-19 scams and fraudulent websites.
- ❏ Ensuring secure use of Wi-Fi, both at home and in public.
- ❏ Avoid using company computers for personal email, file sharing sites, or social media.
- ❏ Not copying work files or information to personal devices, including home network drives and personal online storage.
- ❏ Muting or shutting down in-home digital assistants that may continuously record nearby conversations.
- ❏ Not permitting family members or others to use company-provided equipment, including laptops and phones.
- ❏ Eliminating default home Wi-Fi router passwords and performing other home security checks.
- ❏ Confirming screen locks are enabled to ensure workstations are secured when not in use.
- ❏ Never leaving laptops and mobile devices unattended in public spaces or unlocked at home.
- ❏ Using company-approved cloud services or data center storage instead of local storage, for sensitive information such as personally

identifiable information, protected health information, financial data, and Intellectual Property.
- ❏ Avoiding the use of USB sticks and other removable storage.

Supply Chain

Anticipate how entities on which your business depends — cloud, network infrastructure providers, and others — may be affected by COVID-19 disruptions, and develop resiliency options.

Compliance Expectations Have Not Changed!

- ❏ Allocations decisions outside the norms;
- ❏ Insider Trading Reviews;
- ❏ Personal Trading Activity, looking for new conflicts of interest;
- ❏ Any deviations from the Valuation Policy and process.

For Regulatory Compliance Considerations

- ❏ Do you need to do a quick review with your business departments to see if they have any issues arising from outdated policies and procedures?
- ❏ Do you need to refresh your risk assessment?
- ❏ Are you current on all regulatory requirements, especially Reg BI and Form CRS?
- ❏ Is your Form ADV disclosures up to date as a result of any changes from the virus?
- ❏ Maintain Proper Books and Records

Contents of Written Worksite Specific Plan

- ❏ The person(s) responsible for implementing the plan.
- ❏ A risk assessment and the measures that will be taken to prevent spread of the virus.
- ❏ Training and communication with employees and employee representatives on the plan.
- ❏ A process to check for compliance and to document and correct deficiencies.
- ❏ A process to investigate COVID-cases, alert the local health

department, and identify and isolate close workplace contacts of infected employees until they are tested.

Topics for Employee Training

- ❏ Information on COVID-19, preventing spread, and who is especially vulnerable.
- ❏ Self-screening at home, including temperature and/or symptom checks using CDC guidelines.
- ❏ The importance of not coming to work if employees have a frequent cough, fever, difficulty breathing, chills, muscle pain, headache, sore throat, recent loss of taste or smell, or if they or someone they live with have been diagnosed with COVID-19.
- ❏ When to seek medical attention.
- ❏ The importance of hand washing.
- ❏ The importance of physical distancing, both at work and off work time.

Individual Control Measures & Screening

- ❏ Symptom screenings and/or temperature checks.
- ❏ Encourage workers who are sick or exhibiting symptoms of COVID-19 to stay home.
- ❏ Encourage frequent handwashing and use of hand sanitizer.
- ❏ Provide disposable gloves to workers using cleaners and disinfectants if required.
- ❏ Consider gloves a supplement to frequent hand washing for other cleaning tasks such as handling commonly touched items or conducting symptom screening.
- ❏ Strongly recommend cloth face covers.
- ❏ Close or increase distance between tables/chairs in break rooms or provide break areas
- ❏ in open space to ensure physical distancing.
- ❏ Communicate frequently to customers that they should use face masks/covers.

Cleaning and Disinfecting Protocols

- ❏ Perform thorough cleaning in high traffic areas.

- ❏ Frequently disinfect commonly used surfaces and personal work areas.
- ❏ Clean and sanitize shared equipment between each use.
- ❏ Clean touchable surfaces between shifts or between users, whichever is more frequent.
- ❏ Equip shared spaces with proper sanitation products, including hand sanitizer and sanitizing wipes and ensure availability.
- ❏ Ensure that sanitary facilities stay operational and stocked at all times.
- ❏ Use products approved for use against COVID-19 on the Environmental Protection Agency (EPA)-approved list and follow product instructions and OSHA requirements.
- ❏ Provide time for workers to implement cleaning practices before and after shifts and consider third-party cleaning companies.
- ❏ Install hands-free devices if possible.
- ❏ Consider upgrades to improve air filtration and ventilation.

Physical Distancing Guidelines

- ❏ Implement measures to physically separate workers by at least six feet using measures such as physical partitions or visual cues (e.g., floor markings, colored tape, or signs to indicate to where workers should stand).
- ❏ Reconfigure office spaces, cubicles, etc. and decrease maximum capacity for conference and meeting areas.
- ❏ Adjust in-person meetings, if they are necessary, to ensure physical distancing.
- ❏ Stagger employee breaks, in compliance with wage and hour regulations, if needed.
- ❏ Reconfigure, restrict, or close common areas and provide alternatives where physical distancing can be practiced.
- ❏ Limit the number of individuals riding in an elevator and ensure the use of face covers.
- ❏ Utilize work practices, when feasible and necessary, to limit the number of employees at the office at one time, such as telework and modified work schedules.

Food For Thought

Companies across the economy are considering a permanent shift to remote work in the aftermath of the coronavirus outbreak, following the lead of technology-sector giants. This is going to add to the cybersecurity risks we are already seeing explode.

Confidential Information. Be very careful and be sure staff is aware that video conversations may not be as secure as you think so if you are going to discuss any confidential information or information that could be deemed to be material nonpublic information, be sure you have those conversations in a secure manner.

OutSecure Inc. is helping clients create strategic security roadmaps. Our over 20 years of creating security programs in Fortune 500 has shown that without a strategy any security spend is money wasted and does not achieve risk mitigation.

OutSecure specializes in Establishing or enhancing Cyber Program, Policies, Incident Response Plan and Cyber Personnel Training Our unique team of experts and technology partners are helping companies survive and be profitable in constantly evolving risks to information, cloud implementations and from emerging technology such as Internet of Things and Artificial Intelligence.

This new operating environment will persist for the foreseeable future and we all have to learn and adapt.

For any compliance-related issues, please contact **Todd Spillane** at 832-326-9073 or at todd.spillane@mercurycrs.com
For any cybersecurity-related issues, please contact **Pamela Gupta** at 203-816-8061 or at pamela.gupta@outsecure.com