KING & SPALDING

CRISIS PRACTICE

Coronavirus

MARCH 23, 2020

For more information, contact:

Phyllis Sumner
+1 404 572 4799
psumner@kslaw.com

Robert Hudock
+1 202 626 5521
rhudock@kslaw.com

Scott Ferber
+1 202 626 8974
sferber@kslaw.com

Kim Roberts
+44 (0) 20 7551 2133
kroberts@kslaw.com

Anush Emelianova
+1 404 572 4616
aemelianova@kslaw.com

King & Spalding

Atlanta
1180 Peachtree Street, NE
Atlanta, Georgia 30309-3521
Tel: +1 404 572 4600

Washington, D.C.
1700 Pennsylvania Ave NW
Washington, D.C. 20006
Tel: +1 202 737 0500

Cybersecurity Resiliency in the face of COVID-19

Since the December 2019 outbreak of the novel coronavirus (COVID-19), the virus has spread across the globe, resulting in significant health concerns, deaths, and disruptions to businesses and markets worldwide. For many organizations, existing data privacy and security strategies did not factor in pandemic and public health crises contingencies, including maintaining resilient operations while the vast majority of personnel and third party partners are working remotely. Now more than ever, organizations must ensure they are on high alert for new vulnerabilities and the operational challenges that remote working brings. This requires consideration of legal obligations and risks across jurisdictions, good judgment, and a clear and practical response strategy.

NEW VULNERABILITIES & PRIVACY CONCERNS

As organizations shutter non-essential operations and migrate to remote working arrangements, with their peers, supply chain, and customers doing the same, they must identify and appropriately respond to the unique data privacy and security concerns being created by this public health emergency. COVID-19 related malware, disinformation campaigns, and phishing and ransomware schemes are already being reported, including an app claiming to provide access to a map of real-time virus-tracking but actually containing ransomware. Widespread remote working can lower guards -- organizationally and at the individual employee level. Remote working also creates privacy challenges because of sensitive health information implicated by this emergency. Even with

most personnel already on remote work status, organizations can still take steps to reduce risk.

RISK MITIGATION

- **Increase vigilance in protecting information**. Require, remind, and establish enforcement process to ensure remotely working personnel:
    - only use company provided email, mobile apps, cloud storage, and applications;
    - refrain from emailing organization information to personal emails;
    - avoid using unsecure public WIFI;
    - have a secure, sufficiently complex home router password;
    - refrain from working on sensitive matters in public spaces;
    - safeguard sensitive information (in paper or electronic form) from third parties;
    - use only a cabled connection to a company-issued computer, when printing or scanning; and
    - protect files and maintain them securely so they are not left in the open, on personal computers, in shared spaces, accessible by cloud services, or maintained in other unprotected ways.
- **Heighten sensitivity to COVID-19 related cyber schemes**. Regularly advise personnel to be on alert for COVID-19 related ransomware, phishing, and other fraud schemes and to take the following precautionary measures:
    - scrutinize each and every email;
    - confirm through authorized company channels any “official” email purporting to be about COVID-19;
    - maintain ongoing telephonic communication with known contacts at third party partners (vendors, suppliers, customers) to reduce the risk of unauthorized changes to bank account payment processes by malign actors; and
    - report all suspicious messages and attachments (before clicking) to the appropriate IT Point Of Contact (POC).
- **Minimize and control collection of PII and PHI.** Collect the least amount of Personally Identifiable Information (PII) and Protected Health Information (PHI) necessary, and when doing so, only through controlled, authorized mechanisms.[1] Organizations should take the following protective steps:
    - Alert employees to the do’s and don’ts of PII and PHI sharing in the context of new work routines;
    - Ensure the organization has a secure, protected method for receiving and handling PII and PHI and responding to employees’ requests and inquiries, including identifying a dedicated POC for PII/PHI collection; and
    - Establish an escalation plan to address PII/PHI spillage and unauthorized access.
- **Prepare for the workforce return.** Once the public health emergency subsides, organizations will need to be ready for an orderly return of their remote workforce and should start planning now, including whether the organization will reintegrate all or a portion of the remote workforce. Organizations should develop protocols to:
    - Securely handle and collect diffusely spread data in line with retention best practices;
    - Reintegrate and safeguard assets that have been out of direct control for an extended period; and
    - Debrief returning employees, as well as personnel who will continue to work remotely, on data privacy and security concerns.

FURTHER TECHNICAL CONTROLS

Guidance[2] issued this month by the Cybersecurity and Infrastructure Security Agency (CISA) and National Institute of Standards and Technology (NIST)[3] offer further technical considerations and recommendations for organizations expanding teleworking programs, including:

- **Review available licenses:** Once an organization exceeds its limited number of Virtual Private Network (VPN) connections because of increased use, no other employee can telework and/or connect remotely. With decreased availability, critical business operations may suffer, including IT security personnel's ability to perform cybersecurity tasks. Determine whether your organization has enough VPN connection licenses and computing resources for remote workers to connect and carry out their responsibilities and if necessary, prioritize who should have access or expand licenses.
- **Secure email:** To better detect and remediate malign email attacks, enable logging, where available, on email platforms. In recent guidance,[4] CISA recommends organizations avoid use of the unencrypted Hypertext Transfer Protocol (HTTP) protocol and configure their email servers to reduce the risk of a phishing attack. For example, organizations should use SPF (Sender Policy Framework) and DKIM (DomainKeys Identified Mail) rules to "watermark" authorized emails, then set a strong DMARC (Domain-based Message Authentication, Reporting & Conformance) policy to reject all nonconforming messages.
- **Secure VPN connections**: As uses of VPNs for telework increases, more vulnerabilities exist and are targeted by malicious cyber actors. Employees who are not familiar with teleworking may also be more likely to make mistakes or inadvertently enable risky functionality. For example, VPN split tunneling allows a user to use one route for some traffic through the encrypted VPN tunnel while other devices or applications access the internet directly. This configuration change will improve perceived performance by the end user but creates more risk for the organization. CISA's Remediate Vulnerabilities for Internet-Accessible Systems[5] offers recommendations on vulnerability detection and remediation. At the enterprise level, NIST recommends that VPN gateways and portals should be protected by a firewall and should run anti-malware software and intrusion detection software. Some organizations also provide teleworkers with VPN gateway, firewall appliance, or other security devices that are configured to enforce the organization's security policies.
- **Patch, Patch, Patch**: As VPNs are 24/7, organizations are less likely to keep them updated with the latest security updates and patches. Compliance with appropriate patch management policies and independent verification of patching is key.
- **Implement MFA:** Where an organization does not use multi-factor authentication (MFA) for remote access, the organization is more susceptible to phishing attacks and other unauthorized access incidents. This is especially true where the device being used for remote work is a device owned by the employee and not the employer.
- **Implement telework controls:** NIST recommends implementing telework client device controls that include all local security controls used in the organization's enterprise environment. These controls include: automatic patching of applications and operating systems; encrypting sensitive data; disabling unneeded services; using antimalware software; and enabling a personal firewall.
- **Consider on-site requirements**. To the extent not already identified in the organization's business contingency plan, organizations should clarify which tasks *cannot* be performed remotely to maintain data security and compliance and should develop strategies to address these tasks if the current situation persists. Examples typically include items requiring direct physical maintenance of computing systems, environmental systems needed to keep an

organization's datacenter running, and rebuilding corrupted servers. Systems can fail as time goes by due to the lack of maintenance and increased load.

UPCOMING WEBINAR

King & Spalding will address these pressing issues and risk mitigation strategies in an upcoming Webinar (*Top COVID-19 Data Security Concerns: Today and Beyond*) co-hosted with Global Guardian on March 25, 2020 at 12:00 p.m. (EDT).

---

[1] While the Office for Civil Rights (OCR) of the U.S. Department of Health and Human Services (HHS) announced that it would permit some additional flexibility—OCR will not enforce HIPAA violations arising from healthcare providers' use of remote conferencing services to provide tele-healthcare—it also has reminded companies of its bulletin from February indicating that HIPAA's Privacy Rule was still in effect to limit unauthorized sharing of patient information. *See Notification of Enforcement Discretion for telehealth remote communications during the COVID-19 nationwide public health emergency* (Mar. 17, 2020), https://www.hhs.gov/hipaa/for-professionals/special-topics/emergency-preparedness/notification-enforcement-discretion-telehealth/index.html; *BULLETIN: HIPAA Privacy and Novel Coronavirus* (Feb. 2020), https://www.hhs.gov/sites/default/files/february-2020-hipaa-and-novel-coronavirus.pdf. EU regulators, including the Information Commissioner's Office (ICO), have issued guidance to reassure healthcare bodies and professionals that information governance issues should not be a barrier to effective information sharing to manage the response to the COVID-19 virus. *See, e.g.*, *Data protection and coronavirus: what you need to know*, https://ico.org.uk/for-organisations/data-protection-and-coronavirus/.

[2] *Risk Management for Novel Coronavirus (COVID-19),* https://www.cisa.gov/sites/default/files/publications/20_0306_cisa_insights_risk_management_for_novel_coronavirus_0.pdf.

[3] Additional recommendations for teleworking for the enterprise and for individuals can be found in: *Special Publication 800-114, Revision 1, User's Guide to Telework and Bring Your Own Device (BYOD) Security* (July 2016), http://dx.doi.org/10.6028/NIST.SP.800-114r1; *Special Publications 800-46, Revision 2, Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security* (July 2016), http://dx.doi.org/10.6028/NIST.SP.800-46r2.

[4] *Enhance Email & Web Security*, https://www.cisa.gov/sites/default/files/publications/CISAInsights-Cyber-EnhanceEmailandWebSecurity_S508C-a.pdf.

[5] *Remediate Vulnerabilities for Internet-Accessible Systems*, https://www.cisa.gov/sites/default/files/publications/CISAInsights-Cyber-RemediateVulnerabilitiesforInternetAccessibleSystems_S508C.pdf.