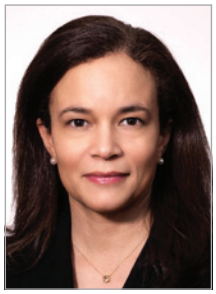
The Legal Intelligencer
THE OLDEST LAW JOURNAL IN THE UNITED STATES 1843-2020
PHILADELPHIA, MONDAY, JUNE 1, 2020 VOL 261 • NO. 105 An ALM Publication

CYBERLAW

Despite COVID-19, Here Are 4 Easy Steps for Data Privacy, Security Compliance

BY JOSHUA A. MOONEY, RICHARD M. BORDEN AND LINDA D. PERKINS
Special to the Legal





MOONEY **BORDEN** **PERKINS**

JOSHUA A. MOONEY *is a partner at White and Williams where he serves as chair of the firm's cyberlaw and data protection group.* **RICHARD M. BORDEN** *and* **LINDA D. PERKINS** *are counsel at the firm. They both focus their practices on cybersecurity and privacy laws.*

The world has changed. Yet, while the COVID-19 outbreak has resulted in a Great Pause for onsite operations, it has not suspended the need for data privacy and security. In fact, it has heightened the necessity of basic and reasonable cybersecurity safeguards both because of the necessary transition to a remote work environment and because of the anticipated collection and tracking of sensitive COVID-19-related data once employees and consumers return onsite. These changes implicate a variety of laws, including employment and consumer laws.

Data privacy and security requirements also remain. For example, many organizations have contractual data security requirements with clients and business partners, some accompanied by substantial indemnity liabilities. As of March 21, the New York SHIELD ACT requires all organizations handling private information of New York residents to have a written and comprehensive data security program. As efforts to delay the legislation have been rejected, enforcement of the California Consumer Privacy Act (CCPA) begins in little over a month.

Yet, data privacy and security need not be viewed as a burden. Nor need it be costly. There are steps an organization may take to harness a data privacy and security (i.e., cybersecurity) program in an efficient and effective manner. A cybersecurity program need not break the bank; nor should it overwhelm a company by diverting valuable resources from a central business mission. An efficient and effective cybersecurity program also may be used to help an organization acquire a valuable competitive edge. The common mistake is to create a complicated process that a company has difficulty supporting or adhering to. Here are four easy steps an organization can take to address the new work and IT environment, albeit guidance from experienced cyber counsel makes these steps even easier:

- **E**stablish a data privacy and security team.
- **A**ssess and identify the new work environment.
- **S**tart adjusting and tweaking your policies and procedures to mitigate the risks and comply with the requirements you identify.
- **Y**our employees, vendors and clients (consumers)—communicate with them. Don't forget employee training.

Establish a data privacy and security team. A central characteristic of any reasonable cybersecurity program is that the organization appoints competent personnel to oversee the program. That person may be in-house, or an organization may look to outside help. Either way, implementing and maintaining a cybersecurity program should not be a one-person job. A best practice is to assemble a team representing a cross-section of the

organization's business, IT, legal and other operation departments to identify, address and remediate risks on a regularly scheduled basis. This team should have the support and involvement of senior management.

Assess and identify the new work environment. COVID-19 has brought changes to the workforce and IT environment that were almost unimagined just a few short months ago. Everyone's work environment has changed, and those changes will persist in the months and perhaps years to come. Just as IT personnel knew their organization's network pre-COVID-19, another "inventory" should be undertaken. Consider the five steps of the NIST Cybersecurity Framework (CSF): identify, protect, detect, respond and recover. Are new devices, especially personal devices, being used? Are servers properly configured? Does your organization need to expand the availability of VPNs or other remote logins? Does your organization need to incorporate multifactor authentication? Are employees using devices, software or platforms that have not been approved by the company? What about your vendor's employees?

Start adjusting and tweaking your policies and procedures to mitigate the risks and comply with the requirements you identify. Data privacy and security is never static. A company should build new procedures or strategies to address any discovered or increased risks, and to correct any errors. After undertaking steps one and two, an organization may identify needed modifications. Consider modeling the program based on the NIST CSF, which is deemed an industry-recognized standard under some data security legislation and regulations. Does the expanded remote workforce require implementation of a data loss prevention (DLP) policy? Has the organization identified employee "work-arounds" that need to be addressed? Do new patching procedures need to be adopted? Is your incident response plan predicated upon a central, onsite presence and need to be adjusted accordingly? Are there security or technical measures that will increase efficiency, business continuity or simply make it easier for personnel to accomplish their work? Remember, if you try to address everything at once, it may be overwhelming and little or nothing will get done. Adjust and tweak within your organization's capabilities. Get help where you need it. Data security is business continuity.

Communicate with your vendors and service providers. Ensure that they have appropriate cybersecurity measures in place.

Your employees, vendors and clients (consumers)—communicate with them. Don't forget employee training. Employee training is essential. Critically, it need not be difficult to accomplish. Make data privacy and security, as well as any IT-related questions or concerns, an agenda item for team meetings. Discuss data requirements—whether legal or contractual—that are required of the company and their own actions. Explain expectations and consequences. Implementation of technical and administrative safeguards can be done inexpensively and with broad effect to tighten data security. Implement requirements for password maturity and strength. Phishing and business email compromise attacks present heightened risks, so ramp up education and testing around them, including through the use of managed service providers. Follow up on lapses with additional training. Be helpful, not punitive. Stress causes people to make mistakes. Training helps reduce those mistakes.

With changes in privacy laws, consumers are entitled to greater disclosures of the collection and use of their information. Ensure that any changes in business operations do not require updates to outward-facing privacy notices. Communicate with your vendors and service providers. Ensure that they have appropriate cybersecurity measures in place. Be sure to track your own contractual cybersecurity obligations with any changes in operations.

A final step. A cybersecurity program must evolve and adapt as new risks and threats emerge. So, plan for next month and next year. An organization's data security and privacy team should meet regularly to help with the program's maintenance and growth. It should plan for incident response exercises and schedule annual assessments, which are required by many contracts and data security laws. Policies and procedures should be examined and amended (if needed) on an annual basis. Personnel should review and acknowledge them. Looking forward and planning ahead enables an organization to better detect, identify and remediate an incident. Taking the time to review and plan appropriately will reduce the time and costs later. And that sure beats looking back at the things that should have been done once an incident occurs. •

Reprinted with permission from the June 1, 2020 edition of THE LEGAL INTELLIGENCER © 2020 ALM Media Properties, LLC. All rights reserved. Further duplication without permission is prohibited. For information, contact 877-257-3382, reprints@alm.com or visit www.almreprints.com. # TLI-06012020-450034