The Legal Intelligencer
THE OLDEST LAW JOURNAL IN THE UNITED STATES 1843-2020
PHILADELPHIA, MONDAY, MARCH 16, 2020 VOL 261 • NO. 51 An ALM Publication

CYBERSECURITY

Cyber Update: Personal Certification by Corporate Executives on the Rise

BY JOSHUA A. MOONEY AND RICHARD M. BORDEN
Special to the Legal


MOONEY


BORDEN

JOSHUA A. MOONEY *is chair of White and Williams' cyber law and data protection group. He advises companies, including members of the insurance and insurtech industries, on data use and ownership, licensing, privacy and security.*

RICHARD M. BORDEN, *counsel in the firm's New York office, focuses his practice on big data governance and the Internet of Things, cybersecurity risk management and technology sourcing and transactions.*

The likelihood of meaningful federal cybersecurity legislation in 2020 remains suspect. Yet, developments in 2019 show that cybersecurity regulation is headed toward a Sarbanes-Oxley model with or without congressional input. The Sarbanes-Oxley Act (SOX) had a significant effect on corporate governance in the United States by requiring public companies to strengthen audit committees, perform internal controls tests, and make directors and officers personally liable for the accuracy of financial statements. For SOX certifications, the act requires that an organization's senior officer personally certify the accuracy of the company's financial reports. A false certification can implicate personal liability. Regulation of cybersecurity is taking a similar approach.

Cyber regulations promulgated by the New York Department of Financial Services (NY DFS), 23 NYCRR Part 500, in 2017 were among the first to require personal certification of a senior officer to compliance of the regulations' requirements. In 2019, cybersecurity regulation veered further toward the Sarbanes-Oxley model, materializing in numerous Federal Trade Commission (FTC) orders, and in a significant, but little spoken about, rule change in the financial services industry when the Securities and Exchange Commission required members of the National Securities Clearing Corp. (NSCC) to undertake cybersecurity confirmations. Growing passage of the model law for insurance data security in multiple states, including Delaware, also incorporates the certification requirement.

The threat of personal liability adds teeth to requirements in regulatory regimes for a written and comprehensive cybersecurity program.

The threat of personal liability adds teeth to requirements in regulatory regimes for a written and comprehensive cybersecurity program. Yet, it has not received much attention. This article briefly addresses these 2019 changes.

THE FTC'S REQUIREMENT FOR ANNUAL CERTIFICATIONS

A recent blog entry posted on the FTC's website identified seven

FTC orders issued in 2019 in connection with enforcement actions that contained self-described departures from prior orders to improve companies' compliance efforts. Discussed in a Jan. 6 post by Andrew Smith, director of the Bureau of Consumer Protection, those "major changes" were greater clarity, increased third-party assessor accountability, and a concerted effort to elevate data security considerations to organization's C-suites and boards of directors.

The last change is critical. The FTC has begun requiring a senior officer of targeted company to provide "annual certifications of compliance" to the requirements set forth under the FTC order to which his organization is bound. For instance, in the action *In the Matter of ClixSense.com*, No. C-6678, the FTC annual certifications as part of the commission's ongoing oversight. The order requires that ClixSense, on an annual basis:

• File "a certification from a senior corporate manager" that the company "has established, implemented and maintained the requirements" of the FTC order.

• Confirm that the company "is not aware of any material noncompliance that has not been corrected or disclosed to the commission."

• Provide a description of any data security incident it sustained during the year.

The certification must "be based on the personal knowledge" of the senior officer or subject matter experts upon whom the senior officer reasonably relies in making the certification.

According to Smith's post, the certification requirement is intended to "force" senior management and the executing officer to "gather detailed information about the company's information security program, so they can personally corroborate compliance with an order's key provisions each year."

THE SEC RULE REQUIRING CERTIFICATION FOR THE NSCC

In October 2019, the NSCC, under the authority of Section 19(b)(1) of the Securities Exchange Act (SEC) of 1934 and corresponding Rule 19b-4, filed with the SEC proposed rule change to require confirmation of cybersecurity program that would require NSCC members, and new applicants, to submit a cybersecurity confirmation at least every two years. On Dec. 9, 2019, the SEC approved the rule, effective immediately.

The NSCC, a wholly owned subsidiary of Depository Trust & Clearing Corp. (DTCC), is a market utility. It plays a prominent role in providing clearance, settlement, risk management and central counterparty services. It also assists to provide a guarantee of completion for virtually all broker-to-broker trades involving equity securities, and corporate and municipal debt securities. Under the Dodd-Frank Act, the NSCC was designated a systemically important financial market utility (SIFMU). As noted in the SEC's approval of the new rule, this designation is significant because it indicates the recognition that a failure of the NSCC by a cyberattack or other means would risk significant liquidity problems spreading among financial institutions and markets, and "thereby threaten the stability of" the U.S. financial system. Thus, this is not a "check-the-box" program. Because cybersecurity programs are evaluated in the context of systems, data and associated risks involved, perfunctory cybersecurity programs—even programs that were deemed sufficient in early 2019—may not satisfy the anticipated requirements of the cybersecurity confirmation.

The cybersecurity confirmation requires member organizations to confirm that they maintain a comprehensive cybersecurity program based on risk assessments aligned with an industry recognized framework, such as NIST's Cybersecurity Framework or the ISO 27001 standard. As specified by the certification form itself, the senior officer must attest that his organization has:

• "Defined and maintains a comprehensive cybersecurity program and framework that considers potential cyber threats that impact the organization and protects the confidentiality, integrity and availability" of the organization's data and information systems.

• "Implemented and maintains written enterprise cybersecurity policy or policies approved by senior management … or board of directors," and that its framework is aligned with industry "best practices and guidelines."

• If using third-party services, "an appropriate program to evaluate the cyber risks and impact of those third parties, and to review the third-party assurance reports."

• A "cybersecurity program and framework that protects the segment of the Company's system that connects to and/or interacts with NSCC."

• An "established process to remediate cyber issues identified to meet regulatory and statutory requirements."

• "A comprehensive review of the cybersecurity program and framework has been conducted by one of the following": itself, if it also has filed and maintains a certificate of compliance under the New York DFS Cyber Regulations, a regulator who assesses the organization's cybersecurity programs; an independent organization with relevant cybersecurity expertise; or an independent internal audit function reporting directly to the organization's board of directors.

The confirmation also must affirm that the organization's "cybersecurity program's and framework's risk processes are updated periodically based on a risk assessment or changes to technology, business, threat ecosystem and regulatory environment." The new rule requires that the NSCC need only provide 180 days' advanced notice of a required cybersecurity confirmation.

THE INSURANCE DATA SECURITY ACT

At the close of 2017, the National Association of Insurance Commissioners (NAIC) promulgated the draft of a Model Law on Insurance Data Security (the act). With the final draft borrowing heavily from the NY DFS cyber regulations, the model law established data security standards and a regulatory framework requiring insurers and other organizations regulated by a state's insurance regime to develop and implement a comprehensive data security (or cybersecurity) program. Five more five states, including Delaware, enacted the model law in 2019.

In each state, the act creates due diligence requirements for insurers relating to their third-party vendors and service providers, including law firms, and requires senior executives and directors to become involved in their organization's cybersecurity framework. The act requires domiciled insurers or producers to report cybersecurity events, including data breaches, to the state's respective insurance commissioners, and empowers the state agencies with investigatory authority and responsibility for violations of the act. In each state, the act also requires certification of compliance to be filed annually with the commissioner of insurance.

WHERE ARE WE HEADED?

The threat of personal liability for the executive officer attesting to cybersecurity compliance increases the stakes for any organization. The FTC has a well-documented history of enforcing its orders in data privacy and security matters. While it is yet unclear as to the level and form of enforcement of these NSCC's cybersecurity confirmation, the Insurance Data Security Act, no senior executive wishes to be charged with lying to a regulator.

Greater pressure from the specter of personal liability will have a ripple effect, especially in the context of cyber-risk management of organizations' third-party vendors, such as brokers, accountants and law firms. Such organizations may begin requiring similar certifications and embed strict data privacy and security requirements in their vendor and supplier contracts. In fact, some already do. This is the intended effect. •