New York Law Journal

NEW YORK LAW JOURNAL SPECIAL REPORT

An ALM Publication

Cybersecurity

WWW.NYLJ.COM

VOLUME 267—NO. 43

MONDAY, MARCH 7, 2022

Never Break the Chain: **Software Supply Chain** Risks and Solutions

BY JUD WELLE AND DAVID KANTROWITZ

Over the past year, cyber incidents have dominated the headlines and, in turn, are causing sleepless nights for boards, C-level executives, and their legal counsel. In the wake of hospitals, food producers, oil pipelines, and companies across all sectors being disrupted by ransomware attacks, the Biden administration has declared that contending with cyber incidents is "essential to national and economic security[.]" Executive Order on Improving the Nation's Cybersecurity, E.O. 14028 (May 21, 2021).

Regulatory and other government agencies have received the message and are shifting into high gear with new initiatives and actions to drive improvements in cybersecurity practices, which were for many years left to the private sector to manage.

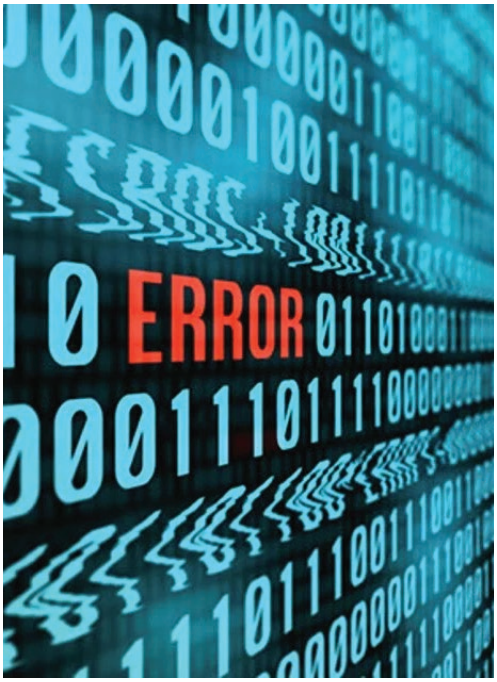
JUD WELLE *is a partner in Goodwin Procter's data, privacy & cybersecurity practice and complex litigation & dispute resolution practice.* DAVID KANTROWITZ *is a partner in the firm's complex litigation & dispute resolution practice and a member of the firm's data, privacy and cybersecurity practice and the firm's financial industry group.*

Against these looming harms and rising expectations, *software supply chain risks* have broken into the mainstream, largely due to a series of highly publicized incidents over the past year. (The most notable of these incidents involved network monitoring software produced by SolarWinds and an open-source logging utility incorporated into an array of applicable and services known as "Log4j.") As a result, cyber regulators have taken notice and advised companies to act on this risk, which is often managed by IT professionals without meaningful input or involvement from legal counsel or senior management.

In this article, we examine software supply chain risks, analyze legal and compliance requirements arising from New York's cyber laws, and offer recommendations to move forward on this area of critical risk that is often neglected or, worse, ignored.

The Digital Supply Chain Problem

It is virtually impossible to operate in today's interconnected world without heavy reliance on software and service platforms developed and maintained by third parties.



© ADOBE STOCK

Once placed into service, both must be closely monitored because, over time, their latent flaws are discovered and become widely known among both information security professionals and cyber threat actors. For the latter group, those vulnerabilities are the cyber equivalent of finding a "golden ticket" to Wonka's Chocolate Factory. They provide the means (or "attack vector" in cyber-speak) for bad guys to worm their way into a company's network.

Most of the time, vulnerabilities are introduced into the software and platforms through inadvertence in

the ordinary course of development, against the backdrop of tight deadlines to debut a new service or add features to existing ones. In the rarer but more troubling cases, malicious actors sneak vulnerabilities into software and platforms right under the noses of the developers and providers. Whatever the origin, companies face serious challenges mitigating the risks that flow from exploitable bugs and "backdoors" in their software solutions.

Legal Analysis

In New York, the legislature and its financial regulator have issued requirements regarding cybersecurity: The Stop Hacks and Improve Electronic Data Security Act (SHIELD Act) (NY Gen. Bus. §899-bb) and the New York State Department of Financial Services Cybersecurity Regulation (the NYDFS Regulation) (23 NYCRR Part 500). These laws cover a wide range of businesses, with the SHIELD Act targeted to businesses that own or license computerized data belonging to New York residents, and the NYDFS Regulation covering companies that operate under a license or similar authorization under New York's banking, insurance, or financial services laws. Here, we are less concerned about *who* is covered, and more interested in *what* the laws say about measures to contend with software supply chain risks.

The NYDFS Regulation, which took effect on March 1, 2017, was and remains groundbreaking in its imposition of heightened cybersecurity standards on businesses. Even so, the NYDFS Regulation's requirements are highly generalized requirements as it pertains to software supply chain risks. The main requirement is that covered companies have written policies and procedures to assess and mitigate cyber risk arising from "Third Party Service Provider(s)," a defined term in the regulation. See NYCRR §§500.1(n), 500.11. With that said, the NYDFS Regulation does not specifically "call out" software supply chain risk. Furthermore, what obligations the NYDFS Regulation does impose relating to third-party cyber risks only cover those third parties that interact with certain defined categories of sensitive information. See NYCRR §§500.1(g), (n). This gap is critical because any software or platform used by a business can create a significant risk of a crippling cyber attack, not only those used to store or process sensitive data. While the NYDFS Regulation itself may be more circumscribed, the Department's statements in the wake of recent incidents suggest that businesses should have robust controls and processes for addressing software supply chain risks. See Report on the SolarWinds Cyber Espionage Attack and Institutions' Response (April 2021); Industry Letter re: Log4j Vulnerability (Dec. 17, 2021); see also FTC Warns Companies to Remediate Log4j Security Vulnerability (Jan. 4, 2022).

The SHIELD Act, which became effective on March 21, 2020, imposes a "reasonable" security requirement on certain organizations, which can be met by implementing a data security program that includes administrative, physical, and technical safeguards to protect the security, confidentiality, and integrity of private information. Like the NYDFS Regulation, the SHIELD Act prompts companies to be vigilant to the risks that arise when relying on third-party service providers. 899-bb(2)(b)(ii)(A)(5). The SHIELD Act also specifically calls attention to software supply chain risks as one of the technical safeguards companies should implement. 899-bb(2)(b)(ii)(B)(1). However, companies are largely left to fashion their own approaches under the SHIELD Act's "reasonable" benchmark.

In short, while New York's cyber laws are among the most innovative and forward-looking in the nation, even they have not kept pace with the dangers lurking in the software supply chain. As a result, companies must look beyond these laws to identify actions and benchmarks for adequate management of these risks.

Recommendations

Businesses can take actions in the following areas to address software supply chain risks.

Obtain Board and Executive Leadership 'Buy-In'. This is the most critical element to any cyber risk program. Without accountability at the top and adequate investment in people, processes, and technology, companies will remain behind the curve in dealing cyber risks. Leader-

ship must champion and establish enterprise-wide cybersecurity and supply chain risk management awareness and promote cybersecurity and supply chain risk management as a business priority.

Cybersecurity Program. Develop and implement robust information security policies including (1) risk assessments, (2) third-party vendor management policies, (3) vulnerability/patch management policies, and (4) incident response plans. These should be drafted (or revised) to include specific standard operating procedures on how to conduct supply chain risk management assessments and ensure security compliance with critical vendors in the supply chain.

Vendor Diligence, Compliance, and Controls. Conduct diligence on each company vendor and establish a standard set of cybersecurity protocols. Diligence should look at information about the vendor's product and supply chain risk management practices and financial ability to provide ongoing vulnerability support. Companies should seek a software bill of materials (i.e., a list of components in a piece of software—both open source and commercial) so they can track their exposure as vulnerabilities come to light. Assess technical security risks prior to onboarding new applications and consider commissioning an independent penetration test or source code review for business critical applications.

Implement a Documented Vulnerability Management Program. Using instructions from the vendor, IT teams should configure software to automatically check for and install patches. Be sure that that software licenses are properly registered with the vendor, including contact information, so that vulnerabilities and mitigation strategies can be communicated on short notice. Follow all vendor instructions to harden software, operating systems, and firmware.

Seek Contractual Protections. Companies engaging vendors can include privacy, security supply chain risk management provisions in service-level agreements that can help manage and mitigate supply chain risk. These should cover physical, technical, and administrative information security standards for vendors and their extended suppliers, as well as measures to audit or obtain assurances regarding the same. Include cybersecurity incident notification timelines, which should extend to notification that a critical vulnerability has been discovered and is being exploited. Finally, companies should establish regular communication channels between itself and its vendors to continually evaluate the vendor's security practices, lest the assessment become a "one and done" exercise.

> Most of the time, vulnerabilities are introduced into the software and platforms through inadvertence in the ordinary course of development, against the backdrop of tight deadlines to debut a new service or add features to existing ones.

Establish Security Controls to Mitigate Impact. Companies can mitigate some supply chain risks by implementing various technical security controls. Limit vendor's access to only the data they need to provide the service. Back up critical company data off network so business operations can be restored in the event of a ransomware attack. Where feasible, apply basic network segmentation to isolate different parts of the enterprise.

Conclusion

Vulnerabilities in trusted software and platforms have always existed, but only recently have they come to be seen as the vector for a debilitating cyber attack. Business leaders and their counsel are best served taking ownership of this challenge and guiding their compliance and information security teams on the issue. The risks are too high and cyber threat actors too cunning to wait for laws to emerge to tell them to do so.