New York Law Journal

NEW YORK LAW JOURNAL SPECIAL REPORT

An ALM Publication

Cybersecurity

WWW.NYLJ.COM

VOLUME 265—NO. 38

MONDAY, MARCH 1, 2021

It's Not Such a Breeze: Assessing Your **Service Providers** After **SolarWinds**

BY MICHAEL R. GRAIF AND CYNTHIA J. LAROSE

In the recent SolarWinds hack, the routine task of downloading a software update turned into a cybersecurity nightmare for over 18,000 organizations including the Treasury Department, AT&T and up to 85% of Fortune 500 companies. See Jason Murdock, *Who Has Been Affected by the Huge SolarWinds Cyberattack So Far?*, Newsweek, Dec. 18, 2020. State sponsored hackers broke into SolarWinds and installed malware in its Orion software update, which gave the hackers back door access to the networks of thousands of customers who installed the update. One constructive outcome of that incident is that it has prompted many businesses to reexamine their vendor risk assessment practices.

New York has a statute that requires that organizations select third-party service providers "capable of maintaining appropriate cybersecurity safeguards." N.Y. Gen. Bus. Law §899 bb, Sec. 2(b)(A)(5). The New York Stop Hacks and Improve Electronic Data Security" (SHIELD) Act (N.Y. Gen Bus. Law §899 aa and bb), which became fully effective in 2020, requires that organizations also document those safeguards in written contracts with those service providers.

Most major organizations already perform diligence on their vendors, especially when sharing proprietary data with vendors like cloud based services, for example. But it is easy to see how third-party application providers like SolarWinds—with whom a business does not voluntarily share data—may not necessarily command the same level of internal scrutiny. The obligation to carefully select third-party service providers under New York's SHIELD Act makes no distinction.

The SHIELD Act applies to "[a]ny person or business which owns or licenses computerized data which includes private information" of a resident of New York. N.Y. Gen. Bus. Law §899 bb, Sec. 2(a). The requirement to select vendors capable of maintaining "appropriate" controls is non-specific. It is intended to require a level of diligence that ensures that service providers, like the business itself, have

MICHAEL R. GRAIF *is an intellectual property member at Mintz and a Certified Information Privacy Professional-US (CIPP-US). He also teaches a social media law course at Penn Law and Benjamin N. Cardozo School of Law.* CYNTHIA J. LAROSE *is chair of Mintz's privacy and cybersecurity practice, a Certified Information Privacy Professional-US (CIPP-US), and a Certified Information Privacy Professional-Europe (CIPP-E).*

reasonable administrative, technical and physical safeguards. The SHIELD Act relaxes the obligation somewhat for small businesses, who can adjust their standards according to the size and complexity of their business and the sensitivity of data they collect.

While a hack like SolarWinds was in some respects inevitable, it highlighted the role of third parties as a weak link in the cybersecurity chain, and focused attention on laws like the SHIELD Act and what diligence activities businesses can and should take when selecting third-party service providers.

Implementing the SHIELD Act's Vendor Risk Management Requirement

Assess Service Providers Using the Standards in HIPAA, GLBA and NY-CRR 500. The SHIELD Act gives guidance as to what would be considered "appropriate cybersecurity safeguards" for third-party service providers. The law states that compliance can be achieved by meeting the corresponding requirements of the Health Insurance Portability and Accountability Act of 1996 (HIPAA), the Gramm-Leach Bliley-Act, or NY-CRR Part 500. Thus, even if a business is not subject to those statutes, it can rely on their specific standards to conduct internal controls-based assessments of its third-party vendors that can assess whether the vendor has "appropriate" controls, consistent with the SHIELD Act.

For example, NY-CRR Part 500, which applies to financial institutions regulated by the NY Department of Financial Services (NYDFS), requires that covered entities ensure that third-party service providers have policies and procedures, including multi-factor authentication, to control access to networks and non-public information. Third-party providers should also have policies and procedures for the use of encryption for non-public information "in transit and at rest." (23 NYCRR Part 500.11). Finally, NY-CRR Part 500 requires that third-party providers make representations and warranties regarding their policies and procedures relating to the covered entity's systems or non-public information. They must also give notice to the covered entity of any cybersecurity event that affects such systems and information. In December, the NY DFS issued an alert in response to SolarWinds to broaden its current requirement for mandatory notification given the "sophistication and persistence of the malware, and the adversary" and asked "any affected institution to file a notice immediately." Cybersecurity Division, Department of Financial Services, Supply Chain Compromise Alert, Dec. 18, 2020.

HIPAA, as modified by the HITECH Act of 2009 (Health Information Technology for Economic and Clinical Health Act, Pub. L. 111-5, 123 Stat. 226), requires that service providers (called business associates) of covered entities maintain the same data security protections as the business itself, and the GLBA uses the same appropriateness standard as does SHIELD. Businesses can and should use those laws and their enumerated criteria for assessing service providers to comply with their obligation under the SHIELD Act.

Diligence Administrative Security. Service providers who meet benchmark standards for technical and physical security should also be assessed for their administrative cybersecurity policies and procedures. The SHIELD Act's appropriateness standard contemplates all three. In the absence of internal processes that ensure that they remain current and effective, the best technical security protections can become outdated in a matter of weeks. New threats must be continually identified, monitored and addressed from a technical perspective. An administrative review of a service provider should include at least the following inquiries about its internal procedures: (1) Does the service provider have a defined process in place to identify, categorize, prioritize, and manage risks to an acceptable level? (2) Does the service provider engage on a regular basis in threat and penetration testing? (3) Does the service provider have a workflow process in place to escalate identified risks for remediation? Technical and physical security processes function best when supported by robust administrative security policies and procedures, all of which should be diligenced in assessing appropriateness under the SHIELD Act.

Monitor External News About Service Providers. A proper risk-based assessment of third-party

service providers begins—but does not end—with a review of the third-party's cybersecurity standards. Organizations must also educate themselves about the health of the service provider's current business, and specifically whether there are any risks associated with its continued viability or its ability to maintain statutorily appropriate standards. To that end, organizations should incorporate business risk intelligence by gathering information about the service provider including news events, financials, layoffs, leadership changes, and lawsuits that can serve as predictors of future vulnerabilities. That information should be used together with the technical controls-based assessment of the service provider's cybersecurity standards to arrive at an overall appropriateness assessment under the SHIELD Act.

Record Interactions With the Service Provider. Once a service provider meets the SHIELD Act's appropriateness criteria and the business selects it as a vendor, it is incumbent on the business and the service provider to cooperate in identifying and sharing information about risks. Ideally, there would be a central risk register that keeps track of all identified risks from internal control failures or external cyber scanning results, and that communicates a risk score both to the business and the services provider. There should also be an audit trail that records all interactions between the business and the service provider, so that if a threat is found, its origin and destination can be easily traced. Finally, when risks that require remediation are identified, the service provider should have compliance-specific reporting to the business showing percent attainment or progress to compliance.

Use Risk Assessments To Address Liability Exposure. Robust vendor risk management programs and risk assessments will inform the business (and its counsel) in contracting practices. Businesses can fine-tune limitations of liability, cost of security incident provisions, and indemnification accordingly to address potential exposure. Ideally, this analysis would be done in the aggregate over all vendor contracts with a view to managing risk business-wide. It should also include a review of cyber insurance coverage and an understanding of what is and is not covered by the policies.

> While a hack like SolarWinds was in some respects inevitable, it highlighted the role of third parties as a weak link in the cybersecurity chain.

Conclusion

Businesses subject to New York's SHIELD Act have a legal duty to ensure that they select service providers with appropriate cybersecurity standards, and to document those standards by contract. That diligence requirement is not always treated with sufficient import by businesses focused on bringing their own administrative, technical and physical safeguards up to standard. As the SolarWinds incident so destructively demonstrated, however, a business's cybersecurity risk is no lower than its weakest defense, which may be to its service providers. While vulnerability to third-party risks may never be fully contained, it can be identified and mitigated by performing the comprehensive diligence of third-party vendors required by New York's SHIELD Act. By informing clients of these obligations, counsel can play a key role in ensuring both legal and technical compliance.