New York Law Journal
Cybersecurity
WWW.NYLJ.COM
An ALM Publication
VOLUME 257—NO. 42
MONDAY, MARCH 6, 2017

Regulatory Oversight of Third-Party Arrangements: **Who's Writing the Contract?**

BY JOHN KENNEDY, MICHELLE DEBARGE AND TIMOTHY WRIGHT

Cybersecurity risk from third-party service providers, vendors, suppliers and contractors (collectively referred to in this article as third-party providers) is a significant source of risk to businesses and professions. According to a recent study of information security practices, 74 percent of companies do not have a list of third-party providers who handle their employee and customer data.[1] Another survey revealed that only 42 percent of businesses even consider vendor risk in their work.[2] Not surprisingly, this lack of attention to third-party providers has consequences. In a 2013 Global Security Report by Trustwave, the authors discovered that out of 450 investigations of data breaches, 63 percent of them were directly linked to a third party providing IT services.[3]

Managing third-party provider risk is plainly integral to an organization's overall cybersecurity risk management program. Responding to the growing recognition of "third-party risk," regulators are sharpening their focus on how businesses manage third-party providers, to the point of mandating (or at least strongly encouraging) specific types of terms in contracts with parties that access or manage a company's systems or data. Regulators are further extending their reach by mandating cybersecurity policy content and certain risk management practices for third-party provider arrangements. The much-discussed new rule pending with New York's Department of Financial Services (the "DFS Rule")[4] is just one of the latest examples of regulators picking up the pen on commercial contracts involving cyber risk and on cyber policies involving third-party providers. As currently worded, the DFS Rule (effective on March 1, 2017) requires financial entities to create written security policies specifically addressing third-party providers. This includes the use of certain contract terms

JOHN KENNEDY *and* MICHELLE DEBARGE *are partners, and* TIMOTHY WRIGHT *is an associate, at Wiggin and Dana.*

requiring third-party providers to establish multifactor authentication and encryption capabilities and to adhere to 72-hours notification requirements following a breach.[5]

The approach of the DFS Rule is a not a new concept in the regulation of private sector data security practices. HIPAA business associate agreements—essentially data handling agreements containing mandatory terms to ensure third-party providers and their down-stream contractors handle protected health information in a manner consistent with the legal obligations that govern HIPAA covered entities[6]—have been a staple of health care industry transactions for many years. The data security requirements of the Gramm-Leach-Bliley Act of 1999, which form the basis of the Safeguards Rule,[7] have long obligated a covered financial services entity to "[r]equire its service providers by contract to implement appropriate measures designed to meet the objectives of these Guidelines."[8] In 2010, Massachusetts became the first state to require businesses processing personal information of state residents to create and implement a written information security policy. The Massachusetts regulation also directs businesses to conduct due diligence on third-party providers that handle personal information and to require contractually that third-party providers implement security measures that mirror the security requirements of the Massachusetts rule as well as applicable federal requirements.[9]

While regulatory focus on third-party provider security risk is not novel, recent regulations and guidance increasingly contain more expansive contractual mandates, as well as substantive risk management obligations for the regulated entity. For example:

• A 2013 Risk Management Guidance for national banks, federal savings associations and their technology service providers issued by the Office of the Comptroller of the Currency lays out, in effect, a template of commercial and legal contract terms that federal auditors would presumably look for in third-party providers' contracts with regulated entities.[10]

• A draft model data security law for the insurance industry would require insurers to contractually obligate providers to give notice of a security breach within three days of its discovery, to indemnify the insurer against losses from incidents, and to provide representations and warranties of compliance "with all requirements."[11]

• A new student data privacy law in Connecticut mandates the inclusion of 10 specific contract terms for service providers of public schools who access identifiable student information, ranging from specific legal compliance representations and security undertakings to data ownership terms and choice of law, and purports to void contracts with school boards that do not conform to these requirements.[12]

• A pending rule by the FDIC and other federal financial regulators includes extensive provisions regarding the oversight and control of "external dependencies" (i.e., third-party providers) through detailed monitoring and controls enforced via contract.[13]

• The U.S. Securities and Exchange Commssion has announced that its cybersecurity examinations will include inquiries into the contractual terms in third-party provider agreements relating to cybersecurity and how organizations are exercising contractual control over third-party risks, including changes during the contract term that may affect security risks.[14] FINRA has issued similar guidance, but with even more detailed suggestions as to appropriate contract terms with third-party providers (including terms addressing data storage, breach notification, audit rights, access controls, use of subcontractors and termination rights).[15]

• A recent FTC guide for businesses makes clear that the FTC expects businesses to execute contracts that include appropriate security commitments by third-party providers who manage or access the business's data or systems and that allow for inspection, monitoring or other verifications that these commitments are being met.[16]

• Some state governments, such as Connecticut, are beginning to specify detailed cybersecurity contracting terms for third-party providers to state agencies.[17]

Does this trend mark the end of cybersecurity commercial contract negotiations, with agency-issued

clauses being mechanically plugged into a cybersecurity "standard terms" exhibit? Not likely. But while the regulations still leave plenty of room for individualized cybersecurity contract terms, practitioners should pay attention to an emerging consensus as to what reasonable cybersecurity measures mean within the four corners of third-party provider contracts.

Companies should be aware of what their regulators expect to see in cyber-related contracts, and so should third-party providers to those companies. Although regulators may not be dictating comprehensive cybersecurity contract terms for private sector commercial arrangements, the parties should be aware that they're not starting with a blank slate either. In many cases, certain minimum terms are required, or at least strongly encouraged. For the sake of efficient negotiations, as well as prudent compliance, lawyers on both sides of the table should know what the applicable regulators would expect to see in the contracts if reviewed as part of an examination or investigation.

Where a third-party provider contract contemplates the provider's access to sensitive, regulated or materially proprietary company information, the collective weight of recent state and federal regulatory guidance on third-party provider cyber risk urges that certain minimum issues be addressed. Baseline terms should address (1) minimum required administrative and technical security undertakings by the third-party provider (which may be specified in detail and/or tied to compliance with agreed upon independent security standards (e.g., ISO 27001, PCI DSS)), (2) audits, inspection and monitoring rights to enable the company and its regulators to verify a third-party provider's compliance with these undertakings and third-party provider obligations to correct deficiencies, (3) controls over the subcontracting of the third-party provider's cyber-related obligations to further sub-tiers, (4) third-party provider duties of notification and cooperation in the event of security incidents, (5) third-party provider commitments (where appropriate) to support a customer's disaster recovery and business continuity requirements, and (6) termination remedies and transition assistance where a third-party provider breaches cybersecurity-related obligations.

Responding to the growing recognition of "third-party risk," regulators are sharpening their focus on how businesses manage third-party providers, to the point of mandating (or at least strongly encouraging) specific types of terms in contracts with parties that access or manage a company's systems or data.

The increasing specificity of cyber regulations and guidance does not mean that contract negotiations are reduced to checking off the boxes or cutting and pasting "magic language" from regulations and guidance documents. Some regulated businesses may be understandably tempted to take a literalist approach to cybersecurity contract compliance by throwing into contracts only the minimum language referenced in a specific regulatory requirement or recommendation. But most of the regulations and guidance noted here focus more broadly on addressing in contracts certain areas or principles concerning cyber risk. They do not necessarily dictate comprehensive contract language, preempt negotiations, or specify the degree or type of cybersecurity risks the contracting parties in fact face. Moreover, none of these regulations expressly creates a compliance safe harbor simply on the basis of signing a contract that dutifully tracks a regulator's issues checklist. The New York DFS assessment of public comments on the proposed Rule repeatedly acknowledges that effective compliance will turn on whether or not measures adopted by covered entities are tied to the risks actually posed by third-party provider relationships.[18] Accordingly, flexibility and reasonableness under the circumstances continue to be basic compliance principles in the DFS Rule and in similar rules and regulatory guidance documents. Gauging appropriate cybersecurity measures—including contract language—based on an understanding that the *specific risks* associated

with the third-party provider relationship is at least as important as following the bouncing ball in the regulatory text.

In managing third-party provider cyber risk, actions speak louder than words. Some regulatory pronouncements, as noted here, urge businesses to include a variety of specific representations, warranties and covenants from third-party providers as to minimum security measures that will apply to their services or to access to customer systems and data. Many of these recommendations make good sense and are commonly included in negotiated commercial agreements. But these terms alone don't address the basic theme running through most of this new crop of cybersecurity guidelines for vendor risk management: Customers should use the contractual relationship to ensure active, continuous oversight and monitoring of, and reasonable controls over, how a vendor is managing cybersecurity risk. Contract terms that facilitate careful joint governance that is diligently followed in practice are at least as important as well-crafted security promises in the contract.

Depending on the degree of cyber risk inherent in the third-party provider relationship, these risk management and governance terms will include audit and inspection rights, timely performance reports, real-time monitoring mechanisms, periodic risk assessments, change control procedures for adjustments to security measures, incident response and recovery measures, vendor training in customer policies and clear channels for prompt security-related communications between the parties. A useful mantra for contract negotiators who don't want to miss the larger risk management forest for the regulatory trees is the NIST Framework Core: Identify, Protect, Detect, Respond, and Recover.[19] Collectively, these five pillars of the Framework encompass the foregoing risk management and governance activities both under the contract and throughout the contractual relationship, as well as pre-contract measures such as risk assessment and third-party provider due diligence.

Integrate procurement and contract management functions with the organization's broader cybersecurity risk management program. Organizations that rely on third parties to handle critical data and systems will have gaping holes in their cybersecurity risk management if the program does not fully integrate corporate purchasing, RFP issuance and contracting functions with legal, compliance, due diligence and risk management functions. This is presumably why the DFS Rule requires covered entities to create written security policies specifically directed to third party sources of risk. More than just the DFS Rule's prescription of specific contract terms, the real take-away from the regulation and similar new rules is its mandate to put third-party risk front and center in cybersecurity risk management.

1. PricewaterhouseCoopers, PwC Viewpoint on Third Party Risk Management 5 (2013).
2. PricewaterhouseCoopers, US Cybersecurity: Progress Stalled 12 (2015).
3. New York University, Center for Cybersecurity, Third-Party Cyber Risk and Corporate Responsibility 9 (2017).
4. N.Y.S. Dep't of Fin. Servs., Cybersecurity Requirements for Financial Services (Proposed), 23 N.Y.C.R.R. Part 500.
5. Id. §500.03(12) (discussing requirement to address third parties in a cybersecurity policy), §500.11 (discussing requirement to implement third party security policies).
6. 42 U.S.C. §§1320d et seq.; 45 C.F.R. §§164.502(e), 164.504(e), 164.532(d) and (e) (rules covering HIPAA business associates).
7. 15 U.S.C. §6801(b).
8. 12 C.F.R. §30, Appx. B.
9. 201 Mass. Code Regs. §§17.00, 17.03(2)(d).
10. U.S. Dep't of the Treasury, Off. of the Comptroller of the Currency, OCC Bulletin 2013-29 (2013).
11. Insurance Data Security Model Law §G(2) (Preliminary Working Draft 2016).
12. An Act Concerning Student Data Privacy, Public Act 16-189.
13. Enhanced Cyber Risk Management Standards, 82 Fed.Reg. §8172.
14. Off. of Compliance Inspections and Examinations, 2015 Cybersecurity Examination Initiative (2015).
15. The Fin. Indus. Regulatory Auth., Report on Cybersecurity Practices (2015).
16. Fed. Trade Comm'n, Start With Security: A Guide for Business (2015).
17. An Act Improving Data Security and Agency Effectiveness, Public Act 15-142.
18. Assessment of Public Comments for New Part 500 to 23 NYCRR, N.Y. Dep't of Fin. Servs.
19. National Inst. Of Standards And Tech., Cybersecurity Framework (2013).