Remain Vigilant: Managing Cybersecurity Risks in Third-Party Outsourcing Relationships

This article was originally published on February 27, 2014 and is reprinted with permission from *Corporate Compliance Insights*.

by Aaron Oser and Meighan O'Reardon

Aaron M. Oser, Partner
Global Sourcing
+1.202.663.8031
aaron.oser@pillsburylaw.com

Meighan E. O'Reardon, Senior Associate
Global Sourcing
+1.202.663.8377
meighan.oreardon@pillsburylaw.com

Managing third-party suppliers presents significant compliance challenges that often span an organization, raising legal, insurance, human resources and technology concerns, to name just a few. Corporations will continue to wrestle with these risks in the year ahead, but the convergence of external threats, abundance of valuable corporate data and the current regulatory environment has highlighted the importance of corporate cybersecurity practices. Cybersecurity is perhaps one of the hottest topics being discussed in boardrooms today. The Cybersecurity Framework, anticipated legislation and litany of high-profile data breaches have resulted in even more heightened scrutiny.

The landscape for corporate cybersecurity is rapidly changing and outsourced services, including IT and business process services, all stand to be impacted. Corporate stakeholders, particularly in the legal, information security and information technology departments, should be keenly focused on the current cybersecurity climate and the state of cybersecurity across third-party outsourcing agreements.

A significant aspect of this heightened attention on cybersecurity is not only how third-party outsourcing partners are managing security as part of the service they deliver, but also the risk and cybersecurity exposure to an organization from these third-party relationships. Attackers increasingly exploit weaknesses in third-party suppliers' networks to access data and assets from target companies. As a result, having in place the appropriate contractual and governance safeguards with your third-party suppliers is paramount.

Efforts to integrate and manage cybersecurity in outsourcing arrangements should start early. Detailed security assessments and internal cybersecurity stakeholders should be included as part of initial due diligence efforts with selected suppliers. It is important to understand the security processes and tools that proposed suppliers will use as part of the outsourced service, the supplier's vulnerabilities and plans to remediate gaps during the term of the proposed agreement and the plan for the supplier to integrate with existing corporate cybersecurity programs. Also, understanding how the supplier has previously responded

to past incidents and improved its operations as a result is crucial.

Contract documentation should include meaningful cybersecurity provisions related to liability and indemnification for incidents and identify the security policies and procedures that the supplier will be expected to comply with during the term. Ideally, contracts should support liability and indemnification provisions that align with the value of the data exposed to the third-party supplier, not simply derivatives of the contract value. Including adequate audit and risk assessment provisions for regular risk assessments and remediation plans (annual at a minimum), of the supplier's operations is also highly recommended.

It is important to remain mindful of proposed cybersecurity legislation – at both the federal and state levels – that may need to be accounted for in outsourcing agreements. Compliance professionals should continue to monitor the proposed landscape of legislative and regulatory changes. Accounting for requirements in third-party agreements to accommodate new cybersecurity laws will be critical.

Finally, and perhaps most importantly, governance models that allow corporations to manage the security functions of individual suppliers as well as the full portfolio of suppliers in a holistic fashion will become increasingly important over the next year. The ability to respond quickly to incidents but also make the appropriate strategic risk management decisions related to cybersecurity will be a defining characteristic of a strong corporate cybersecurity program.

Compliance managers and in-house counsel should remain keenly focused on cybersecurity during the next year when negotiating new agreements, amending existing contracts or participating in ongoing governance activities with current service providers. Proactively addressing cybersecurity risks by incorporating security considerations early in the contracting process and defining more appropriate services descriptions, service levels and interaction/governance frameworks can help limit cybersecurity exposures in the first place.

Author Biographies

Mr. Oser is the firmwide leader of the law firm's Global Sourcing practice, the largest customer focused sourcing practice in the world with over 75 professionals, providing integrated legal and consulting services. He devotes a significant portion of his practice to counseling clients on large-scale, complex strategic information technology and business process outsourcing, transformational outsourcing, development, integration, facilities management and telecommunications transactions. He has negotiated and documented a wide variety of technology-related transactions including information technology, business process and transformational outsourcing arrangements; turn-key system acquisition and systems integration agreements; software licensing, development, maintenance and distribution contracts; multimedia agreements; professional services arrangements; and hardware acquisition and maintenance agreements. http://www.pillsburylaw.com/aaron-oser

Ms. Meighan O'Reardon is a senior associate focusing on technology transactions, including information technology and business process outsourcing transactions; software licensing and development arrangements; intellectual property contracts; and other related corporate transactions. Ms. O'Reardon also regularly advises on data use and privacy matters. http://www.pillsburylaw.com/meighan-oreardon

Pillsbury Winthrop Shaw Pittman LLP | 1540 Broadway | New York, NY 10036 | 1.877.323.4171
ATTORNEY ADVERTISING. Results depend on a number of factors unique to each matter. Prior results do not guarantee a similar outcome.
© 2014 Pillsbury Winthrop Shaw Pittman LLP. All rights reserved.