The Sedona Conference Journal

Volume 17 | Number 2 2016

A Clear and Present Danger: Mitigating the Data Security Risk Vendors Pose to Businesses

John Thomas A. Malatesta III & Sarah S. Glover

Recommended Citation:

John Thomas A. Malatesta III & Sarah S. Glover, A Clear and Present Danger: Mitigating the Data Security Risk Vendors Pose to Businesses, 17 Sedona Conf. J. 761 (2016).

For this and additional publications see: https://thesedonaconference.org/publications

The Sedona Conference Journal® (ISSN 1530-4981) is published on an annual or semi-annual basis, containing selections from the preceding year's conferences and Working Group efforts. The Journal is available on a complimentary basis to courthouses and public law libraries and by annual subscription to others ($95; $45 for conference participants and Working Group members). Send us an email (info@sedonaconference.org) or call (1-602-258-4910) to order or for further information. Check our website for further information about our conferences, Working Groups, and publications: www.thesedonaconference.org.

Comments (strongly encouraged) and requests to reproduce all or portions of this issue should be directed to:
The Sedona Conference,
301 East Bethany Home Road, Suite C-297, Phoenix, AZ 85012 or
info@sedonaconference.org or call 1-602-258-4910.

The Sedona Conference Journal® designed by MargoBDesignLLC at www.margobdesign.com or mbraman@sedona.net.

Cite items in this volume to "17 Sedona Conf. J. _____ (2016)."

A CLEAR AND PRESENT DANGER: MITIGATING THE DATA SECURITY RISK VENDORS POSE TO BUSINESSES

*John Thomas A. Malatesta III & Sarah S. Glover**
Maynard Cooper & Gale
Birmingham, AL

> *"It is abundantly clear that, in many respects, a firm's level of cybersecurity is only as good as the cybersecurity of its vendors."*
>
> *-Benjamin Lawsky, New York State Department of Financial Services Superintendent, Oct. 21, 2014.*[1]

Target. Home Depot. T-Mobile. What do these high-profile data breaches have in common? They were all vendor[2] breaches. That is, a third-party service provider served as the vehicle to these organizations' customer data. Vendors are consistently cited as a primary cause of data breaches, and third-

* John Thomas ("J.T.") Malatesta is the Chair of Maynard Cooper & Gale's Cybersecurity & Privacy Practice. Sarah Glover is an associate in the group. Their practice at Maynard Cooper focuses on advising companies in the areas of cybersecurity risk management, data breach response, and privacy compliance. J.T. is a NetDiligence® Breach Coach; he guides clients through the immediate and necessary steps following a data breach, including incident response, data breach notification, regulatory inquiries and, if necessary, civil litigation.

1. Letter from Benjamin Lawsky, Former Superintendent of the N.Y. State Dep't of Fin. Servs., to N.Y. Banks on Cybersecurity (October 21, 2014).

2. As used herein, the term "vendor" shall broadly mean any third party with which an organization has an existing or potential business relationship, recognizing that the typical vendor relationship involves the outsourcing of some function or service to another organization.

party involvement remains the highest *per capita* contributor to the cost of a data breach.[3]

Just ask Target. Target reported that the hackers who ultimately stole 110 million customer records in 2013 initially broke into Target's system by using credentials lifted from an HVAC vendor.[4] From this initial access point, the hackers were eventually able to upload their malicious software to Target's point-of-sale systems, and the rest, as they say, is history. Target has reported the cost of dealing with the data breach to total $200 million to date, reflecting $290 million of gross expense partially offset by an insurance receivable of $90 million.[5]

The litany of household-name breaches, along with the evolving regulatory framework governing third-party relationships, emphasize the importance of including vendor management within your enterprise risk management program, and devoting sufficient resources toward combating the cyber risk vendors present to your organization. Simply stated, vendor relationships can no longer be left in the capable hands of Information Technology to manage alone. It has evolved into an enterprise risk, prompting legal, compliance, operational risk,

---

3. *See* PONEMON INSTITUTE, 2016 COST OF DATA BREACH STUDY: UNITED STATES, at 9 (2016); PONEMON INSTITUTE, 2015 COST OF DATA BREACH STUDY: UNITED STATES 10 (2015). Thirty-six percent of businesses surveyed by the Ponemon Institute in 2014 reported data breaches caused by third party errors, glitches, or misuse. PONEMON INSTITUTE, 2014 COST OF DATA BREACH STUDY: UNITED STATES 9 (2014).

4. Brian Krebs, *The Target Breach, By the Numbers*, KREBSONSECURITY (May 6, 2014, 12:24 EST), http://krebsonsecurity.com/2014/05/the-target-breach-by-the-numbers/; Brian Krebs, *Target Hackers Broke in Via HVAC Company*, KREBSONSECURITY (Feb. 5, 2014, 13:52 EST), http://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/.

5. Target Corp., Quarterly Report (Form 10-Q), at 11 (November 25, 2015).

executive management, and other business segments to augment the risk management efforts aimed at third-party service providers.[6]

The risk vendors present to the security of an organization's sensitive data is two-fold: 1) the vendor itself could maintain the data (e.g., the medical transcription service that maintains a covered entity's patient records); or 2) the vendor does not maintain sensitive data, but could provide an access point to that data (e.g., the unidentified vendor whose stolen login credentials were used to gain perimeter access to Home Depot's systems),[7] creating potential exposure of an entity's customer and employee personal information, financial and proprietary business information, and intellectual property. Benjamin Lawsky, the first superintendent of New York's Department of Financial Services, observed that "third-party firms can provide a backdoor entrance to hackers who are seeking to steal sensitive . . . customer data."[8] This operational reality counsels in favor of extending vendor risk management to an organization's entire roster of vendors, contrary to the traditional model of only focusing on those vendors who specifically handle cus-

6. *See, e.g.*, National Association of Insurance Commissioners, *Principles for Effective Cybersecurity: Insurance Regulatory Guidance* (2015), http://www.naic.org/documents/committees_ex_cybersecurity_tf_final_principles_for_cybersecurity_guidance.pdf ("Cybersecurity transcends the information technology department and must include all facets of an organization.").

7. The Home Depot, *The Home Depot Reports Findings in Data Breach Investigation* (Nov. 6, 2014), http://ir.homedepot.com/news-releases/2014/11-06-2014-014517315.

8. N.Y. State Dept. of Fin. Servs., *NYDFS Report Shows Need to Tighten Cyber Security at Banks' Third-Party Vendors* (April 9, 2015), http://www.dfs.ny.gov/about/press/pr1504091.htm.

tomer data. The New York State Department of Financial Services (NYDFS), for example, found that the majority of banks it surveyed performed security risk assessments of their high risk vendors, such as payment processors, but did not conduct the same level of oversight for those vendors categorized as low-risk, such as office suppliers and printing companies, or for professional service providers, such as legal counsel or independent consultants.[9]

Increased regulatory scrutiny in this area further compels a more comprehensive approach to vendor management. The Payment Card Industry Security Standards Council published new guidance on third-party service provider security in August of 2014. The Securities and Exchange Commission's (SEC) Office of Compliance Inspections and Examinations (OCIE) conducted a cybersecurity preparedness examination of more than 100 registered broker-dealers and investment advisors in 2014 that focused in part on third-party risk.[10] This was followed by the OCIE's 2015 Cybersecurity Examination Initiative, which again places vendor management on the short list of topics to receive heightened scrutiny.[11] Most recently, on September 13, 2016, the NYDFS proposed new cybersecurity regulations that would obligate financial institutions to, among other things, implement and maintain a written cybersecurity policy that addresses a number of areas, including vendor and

9. N.Y. State Dept. of Fin. Servs., *Update on Cyber Security in the Banking Sector: Third Party Service Providers*, at 3 (2015), *available at* http://www.dfs.ny.gov/reportpub/dfs_rpt_tpvendor_042015.pdf.

10. UNITED STATES SECURITIES AND EXCHANGE COMMISSION OFFICE OF COMPLIANCE INSPECTIONS AND EXAMINATIONS, CYBERSECURITY EXAMINATION SWEEP SUMMARY, at 1 (2015), *available at* https://www.sec.gov/about/offices/ocie/cybersecurity-examination-sweep-summary.pdf.

11. PCI SECURITY STANDARDS COUNCIL, THIRD-PARTY SECURITY ASSURANCE (2014), *available at* https://www.pcisecuritystandards.org/documents/PCI_DSS_V3.0_Third_Party_Security_Assurance.pdf.

third-party service provider management.[12] In an area of law that is rapidly evolving, and as businesses continue to increase the number and complexity of third-party relationships, organizations large and small would be well advised to get out in front of this issue.

The threat vendors pose to businesses is tangible. Fortunately, so are the steps a business can take to mitigate that threat. The key to vendor management—indeed any cybersecurity preparedness program—is deterrence; there is no guarantee that "doing everything right" will absolutely prevent a data breach, but implementing a comprehensive vendor management program is a formidable way to reduce the cyber risk vendor relationships introduce. This paper will examine how the law charges businesses with overseeing their vendors and how businesses are actually managing (or failing to manage) their vendors today, and it will provide practical guidance on how a business can reduce the cyber risk that vendors present.

CALL OF DUTY—WHAT IS REQUIRED OF BUSINESSES?

The exact vendor management practices that an organization must currently follow depend on the regulatory framework for that organization. Even in heavily regulated industries like financial services and healthcare, however, the law with respect to vendor management is not extensive—at least not yet. Most regulations come down in the form of general charges. The Federal Financial Institutions Examination Council's (FFIEC) regulations implementing the Gramm-Leach-Bliley Act (GLBA) with respect to banks and other FFIEC-regulated financial institutions exemplify the three basic requirements and/or best practices that businesses should follow:

12. N.Y. State Dep't of Fin. Servs, Proposed 23 NYCRR 500, § 500.03, *available at* http://www.dfs.ny.gov/legal/regulations/proposed/rp500t.pdf.

1. Exercise appropriate due diligence in selecting your service providers;
2. Require your service providers by contract to implement appropriate measures designed to meet the objectives of controlling regulatory guidelines and industry best practices; and
3. Where indicated by your risk assessment, monitor your service providers to confirm that they have satisfied their obligations . . . .[13]

These three pillars of vendor management—due diligence, contractual negotiation, and monitoring—are fleshed out below in the "battle plan" for businesses.

The legal obligations in other industries mirror the FFIEC guidelines. For example, the Health Insurance Portability and Accountability Act (HIPAA) provides that "a covered entity may permit a business associate [i.e., vendor] to create, receive, maintain, or transmit electronic protected health information on the covered entity's behalf only if the covered entity obtains satisfactory assurances, in accordance with § 164.314(a), that the business associate will appropriately safeguard the information."[14] The U.S. Department of Health and Human Services has promulgated guidance on how to comply with this general charge, providing sample contractual language to be inserted in a covered entity's contracts with its vendors who handle protected health information.[15]

---

13. Appendix B, Interagency Guidelines Establishing Information Security Standards, 12 C.F.R. § 570, § III(D) (2000).

14. Administrative safeguards, 45 C.F.R. § 164.308(a)(8)(b)(1).

15. U.S. Dep't of Health & Human Servs., *Sample Business Associate Agreement Provisions* (2013), http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/contractprov.html.

Similarly, the National Association of Insurance Commissioners (NAIC) Standards for Safeguarding Customer Information Model Regulation, adopted by 33 states and the District of Columbia, succinctly captures these general requirements, providing that all licensees shall "[e]xercise[] appropriate due diligence in selecting [their] service providers"; and "[r]equire[] [their] service providers to implement appropriate measures designed to meet the objectives of this regulation, and where indicated by the licensee's risk assessment, take[] appropriate steps to confirm that [their] service providers have satisfied these obligations."[16] This sentiment is echoed in the NAIC's Principles for Effective Cybersecurity: Insurance Regulatory Guidance. (Principle 8: "[T]ake appropriate steps to ensure that third parties and service providers have controls in place to protect personally identifiable information.")[17] The new proposed NAIC model regulation actually goes one step further, requiring not only that "licensee[s] shall contract only with third-party service providers that are capable of maintaining appropriate safeguards for personal information in the licensee's possession, custody or control," but also that "the licensee **shall be responsible** for any failure by such third-party service providers to protect personal information."[18]

16. National Association of Insurance Commissioners, Standards for Safeguarding Customer Information Model Regulation, § 8 (2002), *available at* http://www.naic.org/store/free/MDL-673.pdf.

17. National Association of Insurance Commissioners, *Principles for Effective Cybersecurity: Insurance Regulatory Guidance* (2015), http://www.naic.org/documents/committees_ex_cybersecurity_tf_final_principles_for_cybersecurity_guidance.pdf.

18. National Association of Insurance Commissioners, Insurance Data Security Model Law, § 4(F) (2016), *available at* http://www.naic.org/documents/committees_ex_cybersecurity_tf_exposure_mod_draft_clean.pdf (emphasis added).

Non-banking and non-insurance financial institutions likely fall under the catch-all jurisdiction of the Federal Trade Commission (FTC). These financial institutions are subject to the FTC Safeguards Rule implementing the GLBA, which requires businesses to "select service providers that can maintain appropriate safeguards," "make sure [the] contract requires them to maintain safeguards," and "oversee their handling of customer information."[19] Non-financial institutions in less regulated spheres like retail are not subject to specific cybersecurity regulations, but any business engaged in interstate commerce would still be subject to the FTC's jurisdiction under Section 5 of the FTC Act, which the agency has used to prosecute what it deems to be insufficient data security practices, including lack of proper oversight of vendors.[20] Such businesses would, therefore, be well-advised to comply with the FTC Safeguards Rule and corresponding guidance.

The National Institute of Standards and Technology's Framework for Improving Critical Infrastructure Cybersecurity (NIST Framework), promulgated pursuant to an Executive Order of the White House in February 2014, also includes guideposts for vendor management, and is in fact explicitly intended to "provide[] a common language to communicate requirements among interdependent stakeholders," including external

19. Federal Trade Commission, *Financial Institutions and Customer Information: Complying with the Safeguards Rule* (2006), https://www.ftc.gov/tips-advice/business-center/guidance/financial-institutions-customer-information-complying.

20. *See*, *e.g.*, Complaint, Nations Title Agency, Inc., FTC File No. 052 3117, No. C-4161, at 4 (F.T.C. June 19, 2006), *available at* http://www.ftc.gov/sites/default/files/documents/cases/2006/06/0523117nationstitle_complaint.pdf.

service providers.[21] The NIST Framework targets those organizations within critical infrastructure sectors, but provides a helpful roadmap for any business, advising that cybersecurity roles and responsibilities for third-party stakeholders be established and understood by those entities, and that all external service provider activity be monitored to detect potential cybersecurity events.[22]

STATUS REPORT—WHAT ARE BUSINESSES DOING TODAY?

The problem is not that businesses aren't vetting their vendors at all or that they are completely failing to oversee their activities; the general consensus amongst regulators has been that businesses are not doing *enough*. For example, the NYDFS found that 95% of the banking organizations it surveyed conduct specific information security risk assessments of at least their high-risk vendors, and 95% also have information security requirements for third-party vendors.[23] However, that same survey found that fewer than half of the banks required an onsite assessment of their vendors, and 30% did not require their vendors to notify them in the event of a cybersecurity breach.[24] In its examination of fifty-seven registered broker-dealers and forty-nine registered investment advisers, the SEC's OCIE reported similar deficiencies in the area of vendor management in 2015, finding, for example, that only 51% of broker-dealers and

---

21. NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, FRAMEWORK FOR IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY, at § 3.3, *available at* http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf.

22. *Id*. at DE.CM-6, ID.AM-6, PR.AT-3.

23. N.Y. State Dept. of Fin. Servs., *Update on Cyber Security in the Banking Sector: Third Party Service Providers*, at 2–3 (2015), *available at* http://www.dfs.ny.gov/reportpub/dfs_rpt_tpvendor_042015.pdf.

24. *Id*. at 3, 5.

13% of advisers maintain policies and procedures related to information security training for vendors authorized to access their networks.[25] If organizations in highly regulated sectors are falling short when it comes to vendor management, you can imagine how less regulated organizations may stack up.

In its seminal guidance on this issue, useful for businesses in any industry, the Office of the Comptroller of the Currency (OCC) has observed:

> [t]he OCC is concerned that the quality of risk management over third-party relationships may not be keeping pace with the level of risk and complexity of these relationships. The OCC has identified instances in which bank management has:
>
> - failed to properly assess and understand the risks and direct and indirect costs involved in third-party relationships.
> - failed to perform adequate due diligence and ongoing monitoring of third-party relationships.
> - entered into contracts without assessing the adequacy of a third party's risk management practices.
> - entered into contracts that incentivize a third party to take risks that are detrimental to the bank or its customers, in order to maximize the third party's revenues.

25. UNITED STATES SECURITIES AND EXCHANGE COMMISSION OFFICE OF COMPLIANCE INSPECTIONS AND EXAMINATIONS, CYBERSECURITY EXAMINATION SWEEP SUMMARY, at 4 (2015), *available at* https://www.sec.gov/about/offices/ocie/cybersecurity-examination-sweep-summary.pdf.

- engaged in informal third-party relationships without contracts in place.[26]

All organizations need a comprehensive vendor management program to address the foregoing ubiquitous concepts. However, regulators also recognize that vendor management cannot follow a one-size-fits-all blueprint. For example, the OCC has advised that "[a] bank should adopt risk management processes commensurate with the level of risk and complexity of its third-party relationships."[27] The FTC, which espouses a similar view,[28] maintains that its requirements "are designed to be flexible[;] [c]ompanies should implement safeguards appropriate to their own circumstances."[29]

So what should you do?

BATTLE PLAN—WHAT SHOULD BUSINESSES DO?

Regardless of the specific legal requirements—or lack thereof—facing your particular business, effective vendor management should be considered a best practice no matter your industry. In the words of the FTC, "safeguarding customer information isn't just the law. It also makes good business sense."[30]

---

26. OFFICE OF THE COMPTROLLER OF THE CURRENCY, OCC BULLETIN 2013-29, *available at* http://www.occ.gov/news-issuances/bulletins/2013/bulletin-2013-29.html.

27. *Id*.

28. A plan to comply with the Safeguards Rule "must be appropriate to the company's size and complexity, the nature and scope of its activities, and the sensitivity of the customer information it handles." Federal Trade Commission, *Financial Institutions and Customer Information: Complying with the Safeguards Rule* (2006), https://www.ftc.gov/tips-advice/business-center/guidance/financial-institutions-customer-information-complying.

29. *Id*.

30. *Id.*

An effective risk management strategy involves oversight of the vendor throughout the life cycle of the relationship, from due diligence through termination. But, first, a business should conduct an internal risk assessment. Consider: i) taking inventory of where, what kinds, and how much sensitive data lives on and off your company's systems; ii) the access points to your sensitive data; and iii) your company's overall risk appetite. After all, it is hard to appreciate the risk a vendor may present to your data or your systems if you do not have at least a basic understanding of those elements.

Once an internal risk assessment has been performed, your organization will be primed to evaluate vendors. The following considerations, crafted from available regulatory guidance, best practices, and personal experience, cover the most important elements in the vendor management process, though it would be best to make sure you follow all guidance from your primary regulator in this space. This framework can apply equally to the selection and retention of new vendors as well as the review of existing vendors.

Phase 1: Due Diligence

Due diligence in selecting or reviewing vendors should be commensurate with both your organization's risk appetite and the nature of your relationship to the vendor. Consider a tiered approach to vendor management, whereby you categorize each vendor by data security risk to your business. This approach is sometimes referred to as stratification—the placement of vendors with similar risk profiles into tranches of risk. You can then tailor your risk management approach to each tranche. For example, this may inform your thinking about how much cyber liability insurance a vendor may be required to carry.

Below are some action items and considerations when evaluating potential or existing vendors that will help your organization more fully understand the risk presented by a vendor:

- For vendors who will maintain access to your systems, consider the level and frequency of that access (i.e., will they have administrative privileges? If so, they would present a greater security risk).
- For vendors who will be storing or handling sensitive data, consider the type and volume of data you transmit to them.
- Assess the financial soundness and stability of the vendor by reviewing audited financial statements.
- Determine whether the vendor has ever experienced a data breach, and, if so, how the vendor responded and what remedial steps the vendor has taken to prevent a similar breach.
- Request data security customer complaints filed against the vendor.
- Investigate previous data security regulatory enforcement actions and civil litigations.
- Review the vendor's web sites and other marketing materials to assess the adequacy of the vendor's representations regarding data security and privacy.
- Determine whether the vendor has cyber insurance, and, if so, ask to review a copy of the policy. In particular, examine how the sub-limits are structured.
- Evaluate the vendor's information security and incident response programs, including whether they contain the safeguards to protect personal

information you would expect, and how frequently these programs are reviewed and updated.

  - Consider the lack of a formal information security program and/or incident response program as a red flag that the vendor is ill-prepared to provide adequate data security.

- Ask for results from the most recent independent security assessment of the vendor, and any documented remediation actions that resulted from the assessment.

  - If available, review Service Organization Control (SOC) reports and any certification for compliance with internal control standards, such as those promulgated by NIST and the International Standards Organization (ISO).

- Ascertain the extent to which the vendor will rely on subcontractors to perform the contemplated services and whether those vendors are storing that information.
- Ask how often employees receive training on data privacy and security.
- Ensure that the vendor conducts thorough background checks on the employees who will have access to your company's sensitive data.
- Consider an on-site visit to the vendor to more fully understand the vendor's operations and capacity.

Phase 2: Contract Negotiation

The traditional template vendor contract must be modified to address the evolving cyber liability landscape. For example, indemnification and limitation of liability language should explicitly address data breaches. Businesses now need to specify what dedicated amount of cyber liability insurance coverage its vendors are expected to carry (and perhaps even the types and amounts of sub-limits that should be maintained). Parties should clearly outline what notification obligations will be discharged following a security incident, to whom, and when.

Those businesses that find themselves in a regulated environment are now able to use the regulatory guidance that demands improved vendor oversight to exact more negotiation leverage. As regulators continue to fashion guidance about what are and are not sound data security practices, the practical effect is that these concepts will be woven into vendor contracts. In other words, the 800-pound gorilla that used to be able to flex its industry muscle to unilaterally dictate major contractual terms may be losing some ground. The stigma of a data breach is certainly helping too. Explicit data security safeguards (physical, administrative, and technical) are appearing with increasing frequency in lieu of a general mandate to follow "industry standards" in order to provide greater accountability. Vendors are being required to undergo audits and other assessments, often at no additional cost to their business partners, to validate the vendor's data security practices. These have become new contractual norms, in part due to heightened regulatory scrutiny surrounding vendor management.

Here are some particular contract points to consider:

- Clearly define the types of personally identifiable information or other sensitive data that will govern the vendor's contractual obligations.

- Specify the data security safeguards (e.g., encryption, intrusion detection and prevention systems, firewalls, data segregation) that you expect the vendor to utilize.
- Require compliance with applicable data security and data breach notification laws and regulations.
- Require the vendor to notify you immediately if a data breach is suspected.
- Require that the vendor preserve all logs, files, and documents related to any suspected breach.
- Require the vendor to conduct an internal investigation if it suspects a data breach, and/or to cooperate with any investigation by your organization.
- Clearly establish which party bears the responsibility of notification to any customers impacted by a data breach.
- Require the vendor to conduct regular audits and submit reports to your organization.
    - Include the types and frequency of audit reports your organization is entitled to receive from the vendor (e.g., financial, SSAE 16/SOC 1, SOC 2, and SOC 3 reports, and security reviews).
- Retain your organization's right to conduct its own audits of the vendor, or to engage an independent party to perform such audits.
- Consider requiring the vendor to carry cyber insurance, as well as naming your business as an additional insured.
    - The case law is still evolving on this topic, but a general commercial policy will likely not

cover your business in the event of a data breach by a vendor.

- Memorialize background check and training requirements.
- Establish what role subcontractors will have in the performance of the vendor's services, including access to and storage of sensitive data.
- Include an indemnification provision that would require the vendor to fully defend, indemnify, and hold your organization harmless from any and all third-party claims, first-party losses (which should be defined to include data security incident investigation costs and customer and regulatory notification costs), expenses, and reasonable attorneys' fees that it should incur in the event that the vendor (or one of its subcontractors) sustains a data breach.
- Try to eliminate any limitation of liability that puts a cap on the amount of damages the vendor would have to pay if it sustains a data breach (or at least an exception to the cap if the vendor fails to meet legally, contractually mandated, or industry standard data security requirements).
- Provide for termination of the contract if the vendor fails to implement and maintain sufficient data security practices, and/or if the vendor sustains a data breach.
- Require secure disposal of all of your company's sensitive information maintained by the vendor following the conclusion of the business relationship.

Vendor relationships are often the product of multiyear contracts which must typically come up for renewal before new language and requirements can be negotiated. But consider asking for contractual amendments or addendums that speak to these measures now if your organization has the leverage to do so. It is worth noting that some cyber liability policies require the insured to establish that its in-house or outside counsel has reviewed the governing vendor agreement in order to provide coverage for a data breach that is the byproduct of the vendor's acts or omissions.

Further, the contract negotiation process is an excellent way to conduct further due diligence. If you want to see where a vendor may be weak, pay attention to the contractual provisions it pushes back on.

Phase 3: Monitoring

As with the other phases of vendor management, the nature of any ongoing monitoring should align with the risk profile of the vendor. More extensive monitoring may be necessary for those vendors who pose the greatest risk to your organization. If resources allow, it would be beneficial to have dedicated personnel at your organization responsible for monitoring and periodically evaluating the vendor's data security practices. You could also engage an independent consultant to perform this task. Generally speaking, monitoring should mirror the due diligence actions set forth above. Specifically, you should also consider the following:

- Restrict and monitor the vendor's access to your company's systems—allow only as much access as the vendor needs to complete the services provided by the governing contract.

- Consider putting on a security training program for the vendor's employees who will be accessing your company's systems.
- Ensure that the vendor conducts its own ongoing data security training of its employees.
- Ensure that any access credentials provided to the vendor are not being misused or provided to unauthorized persons.
- Conduct regular on-site data security inspections and audits according to the type and frequency set out in the governing contract.
- Ensure that any data security issues that arise during inspections, audits, or otherwise are properly addressed by the vendor.
- Watch out for any customer complaints, regulatory investigations/enforcement actions, or civil litigation brought against the vendor, even if unrelated to your organization or industry.
- Establish that access, use, and/or storage of your sensitive data has been discontinued following termination of the business relationship. Receive written assurances that your sensitive data has been purged.

CONCLUSION

In an environment where the term "data breach" has entered mainstream media and executive management is being sued for failure to give proper oversight to company cybersecurity practices,[31] no business, no matter the size, can afford to ignore or minimize the risk that its vendors present. One analyst writing for *Forbes* described a "Cybersecurity Domino Effect":

31. *See, e.g.*, Complaint, Palkon v. Holmes, Civ. Action No. 2:14-CV-01234 (SRC) (D.N.J. Oct. 20, 2014).

> Here's the fundamental truth: We can no longer worry only about our own organization's network security, because so many networks are interconnected and interdependent. A breach in one can easily affect every company in a supply and delivery chain. In fact, we may only be as secure as the least secure partner with whom we connect.[32]

Don't let one of your vendors be the weak link in the chain.

32. Ray Rothrock, *Why the Cybersecurity Domino Effect Matters*, FORBES (May 18, 2015, 10:00 AM), http://www.forbes.com/sites/frontline/2015/05/18/why-the-cybersecurity-domino-effect-matters/#eecad607ee45.