Cybersecurity and Vendor Risk: The Third-Party Risk Challenge is Here Now

By Matt Kelly

For all the concern about cybersecurity these days, compliance professionals can be thankful for this: it propels vendor risk management up the corporate priority list.

Compliance officers might wish that cybersecurity were still the domain of the IT security team — and once upon a time, it was. Those days are gone. Internet technology has transformed how employees work every day and what vendors do for your company via the supply chain.

Taken together, those facts transform what cybersecurity risk actually is. Passwords, firewalls, packet-sniffer technology, and the like are all part of cybersecurity, and always will be. Fundamentally, however, the risk is about knowing who is handling your company's data, and knowing that you can trust those parties to do so. And with vendors now providing so many services that handle a company's data (a trend that won't change any time soon) that means strong vendor risk management will be crucial for effective cybersecurity.

Indeed, the opening sentence at the top of this paper originally said cybersecurity has propelled vendor risk management up the priority list for the board. While statement is true, concern over cybersecurity has actually had a much broader effect. It has driven vendor risk management up the priority list for everyone: regulators, investors, customers, CEOs, operations executives, and, yes, the board.

From Risk to Business Advantage

One glimpse into regulators' unease over vendors and cybersecurity comes from a report released in December by the U.S. Financial Stability Oversight Council. That report, an annual overview of risks that worry U.S. financial regulators, cites technology vendors to the banking sector as a primary concern:

> *Maintaining confidence in the security practices of third-party service providers has become increasingly important, particularly since financial institutions are often serviced by the same providers. The Council encourages additional collaboration between government and industry on addressing cybersecurity risk related to third-party service providers, including an effort to promote the use of appropriately tailored contracting language.*

More vivid examples come from the world of social media. Consider the case of Facebook providing its user data to Cambridge Analytica, which then integrated that data into its work for the Trump presidential campaign in 2016. Those actions, technically legal or not, have led to litigation from consumer groups, regulators opening formal investigations, and severe reputation damage. (Not to mention a $50 billion drop in Facebook's market value.)

Facebook, however, is only one example of the larger issue: social media companies collecting information about their users, and then allowing app developers or other parties to take that user data and put it toward other purposes — including purposes that the original users might never have understood or supported.

Compliance officers and corporate boards might feel squeezed by that pressure. Instead, let's consider that chain of concern from the regulators' perspective.

The regulator is the first party; seeking to protect the interests of the public, the second party. The public interacts with businesses, which are the third parties in the chain. Those businesses then have vendors of their own, working with the businesses in any number of ways — and the risks those vendors can bring are the cause of alarm.

So when regulators voice worry about tech vendors in the banking sector or app developers working with social media giants, those regulators are trying to tame what is, to them, fourth-party risk.

This is the crucial point for compliance and risk officers to grasp. Your third parties are the fourth parties that concern regulators and consumers so much, because they don't know who those fourth parties are or what risks those parties bring. Regulators and consumers want assurance that your business is keeping their fourth-party risks in reasonable check.

That brings us, inevitably, to this:

the better your firm is at at managing third-party risk, the more attractive you become as a third party yourself.

Your third parties are your customers' fourth parties, and that is where they want assurance.

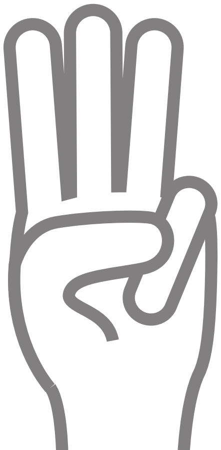
This is why strong vendor risk management is a strategic imperative for the modern business. It allows your business to court more customers, more confidently, because they can get the assurances they want that they are insulated from risks further down the supply chain.

Yes, that point has been true for many risks (corruption, fraud, business continuity, product safety, and more), for many years — but cybersecurity has supplanted those traditional threats as the primary risk, thanks to the speed and scale of Internet technology and its place in the heart of almost every modern business process we have.

So what can compliance officers do to prepare for that cybersecurity-sensitive world?

Three Skills for Effective 'VRM'

Compliance officers can take three steps to hone their company's oversight of vendors' cybersecurity risk. Or, more accurately, compliance programs will need three capabilities to demonstrate effective oversight of those risks.



1

Scoping a SOC audit. SOC audits examine a vendor's cybersecurity controls. ("SOC" stands for "service organization controls.") SOC audits can provide the assurance a company needs that its vendors have effective cybersecurity, if your company includes the right vendor controls in scope of the audit. That is not a simple task.

First, SOC audits exist in two categories. Type I audits merely confirm that a vendor's controls are designed properly at a certain point in time; Type II audits test whether the controls actually work as designed over an extended period of time. Second, all SOC audits measure a vendor's controls against any of five "Trust Service Principles:" security, availability, privacy, process integrity, and confidentiality.

The challenge for compliance and IT security executives will be to identify which principles apply to your vendors, depending on what service they provide to you; and then to scope your SOC audit appropriately. If you include too few principles, you run the risk of under-compliance, overlooking cybersecurity risks you in fact have. Include too many principles and you're in danger of over-compliance, spending money or altering business processes for assurance you don't need.

2

Embracing the NIST protocols. The National Institutes of Standards & Technology publishes cybersecurity control frameworks that any organization can use. Moreover, numerous government agencies, government contractors, and critical infrastructure industries must use them. For example, defense contractors must use the NIST 800-171 standard if they want to bid on government projects. One part of NIST 800-171 requires companies to determine the cybersecurity of their vendors, too.

At first glance the NIST frameworks can seem daunting. They are comprehensive collections of recommended internal controls, and few businesses will need to implement all the controls for their operations. Instead, the challenge will be to identify which controls you do need, given your business processes, vendors, and data collection practices.

3

Showing your work. A wide range of stakeholders will now be seeking more information about how companies handle cybersecurity and data privacy: regulators, audit firms, consumer groups, and more. Even aside from regulators enforcing attention to consumer data, prospective customers and business partners will be just as attentive to security for intellectual property and other proprietary information.

Companies will need an ability to respond to those questions. That means your ability to document and report cybersecurity efforts will be crucial. Risk assessments, vendor audits, service-level agreements, escalation procedures — companies will need a process to document all of them, and a data repository to keep those documents at the ready should a stakeholder ask for them.

In the ideal world, compliance programs should incorporate standardized assessments (such as Shared Assessments' Standard Information Gathering questionnaire, which is mapped to NIST and SOC controls) and cybersecurity ratings providers. This lets you compare your third parties' self-assessment data against outside ratings, which in turn lets you know whether more due diligence, audits, or other steps are warranted. That approach gives you the "single source of truth" and reporting capabilities your boards will be asking for more and more often.

Conclusion

At an abstract level, the three steps above — accurate risk assessments, strong controls, and documentation — are not new. Compliance officers can grasp all those concepts. Indeed, compliance officers relied on those concepts to build anti-corruption programs circa 2010, and Sarbanes-Oxley compliance programs circa 2005. You've been here before. That's the good news.

To apply those concepts to cybersecurity risk in the supply chain, compliance officers will need to forge new alliances with other parts of the enterprise; and develop new policies, procedures, and messaging that stress the importance of vendor risk management.

For example, clearly compliance officers will need to work more closely with IT security and internal audit teams to understand what sort of SOC 2 audits you might want from vendors. Beyond that, however, you'll also need to develop new policies for engaging vendors and monitoring them thereafter — policies that stress the importance of cybersecurity standards to employees who evaluate and work with vendors on a daily basis.

You will, essentially, be using the same tools for vendor due diligence and monitoring that you always have. You'll simply be using them to address a different risk.

Lastly, compliance officers will need to secure executive support for addressing vendor risk, so the rest of the enterprise will embrace the program you propose. You will need to convince the board and CEO that vendor risk is a risk, and one to take seriously.

And as we look at the cybersecurity landscape today, for better or worse, convincing them of that urgency shouldn't be too hard.

About the author

Matt Kelly is a leading compliance industry analyst and consultant, who studies corporate compliance, governance, and risk management issues. He maintains a blog, RadicalCompliance.com, where he shares his thoughts on business issues; and frequently speaks on compliance, governance, and risk topics.
Kelly was named as ‘Rising Star of Corporate Governance’ by Millstein Center for Corporate Governance in inaugural class of 2008; and named to Ethisphere’s ‘Most Influential in Business Ethics’ list in 2011 and 2013.

Kelly was previously editor of Compliance Week from 2006 through 2015. He lives in Boston, Massachusetts, and can be reached at mkelly@RadicalCompliance.com.

About Aravo

Aravo Solutions delivers market-leading cloud-based solutions for managing third party governance, risk, compliance and performance. We help companies protect their business value and reputation by managing the risks associated with third parties and suppliers, and to build business value by ensuring that their third party relationships are optimized.

Since 2000, leading global brands across a diverse range of industries have counted on Aravo for their end-to-end enterprise supplier and third party risk management. Aravo has also distilled this experience and best-in-class technology into rapid time-to-value applications that help companies manage a wide range of programs including: anti-bribery and anti-corruption, responsible sourcing, data privacy, information security, GDPR, financial services regulatory compliance and know your third party programs.

Providing unrivaled regulatory agility and ease-of-use, together with actionable executive reporting, Aravo supports a user base of 124,000 corporate users, managing more than 4.3 million third party users in 36 languages and 154 countries. Aravo is headquartered in San Francisco, with offices and partners across the US, Europe and Asia.

Aravo has been recognized with GRC 20/20's Value Award for Third Party Management for providing measurable value in GRC efficiency, effectiveness and agility, and with the GRC 20/20 Innovation Award for Aravo for GDPR. Aravo was named as a Category Leader with the highest "Completeness of Offering" of any provider in the Chartis RiskTech Quadrant® for Third Party Risk Management Solutions 2017, was named a Challenger in the 2017 Gartner® Magic Quadrant for IT Vendor Risk Management.

Aravo is named a "Leader" in The Forrester Wave™: Supplier Risk And Performance Management Platforms, Q1 2018

Report names Aravo as "the leading SRPM specialist".

Top-ranked for current offering.

Discover why the world's leading brands rely on Aravo Solutions for their Supplier Risk & Performance Management and Third Party Risk Management Programs.

Email: info@aravo.com
Twitter: @aravo
Tel: +1.415.835.7600 [US]
Tel: +44 20 3865 2682 [Europe]

www.aravo.com