riskrecon™

WHITE PAPER

The Seven Deadly Sins of Third-Party Cyber Risk Management

Introduction

The 'seven deadly sins' are a classification scheme established by the Roman Catholic church in the 15th century. It is these seven sins from which they believe all immorality is rooted — pride, greed, lust, envy, gluttony, wrath, and sloth. Similar to the religious seven deadly sins, we have enumerated the seven deadly sins of third-party cyber risk management. It is from these sins that programs fail to lift off the ground, die a slow death, or limit the value they provide to the organization.

First Deadly Sin: Believing that you can outsource your risk

Too many enterprises believe that it is solely the responsibility of the vendor to manage the cyber risk related to the outsourced data and services. This is simply not true. The regulators have consistently made it clear that you can outsource your systems and services, but you can't outsource your risk. In 2008, the Federal Deposit Insurance Corporation stated vendor risk management requirements in this way:

"An institution's board of directors and senior leadership are ultimately responsible for managing activities conducted through third-party relationships, and identifying and controlling the risks arising from such relationships, to the same extent as if the activity were handled within the institution." (www.fdic.gov)

Other regulatory bodies have issued similar guidance — the U.S. Department of Health & Human Services, the European Union, the New York Department of Financial Services, and the Office of the Comptroller of the Currency, among others (See: A regulatory guide to third-party cyber risk).

While your vendor contracts may have financial data breach penalties, or you may have cyber insurance, financial mitigation is not the only risk. You have other risks to consider as well, including regulatory, reputational, and operational risks. You can outsource your systems and services, but you can't outsource your risks.

Second Deadly Sin: Failing to make third-party risk management about business risk management

Business runs on a complex platform of systems and services operated by internal personnel and third parties. Managing cyber risk across these platforms is about managing business risk. Only when the business wants good risk outcomes can good risk outcomes be realized. In third-party risk management, engagement with the business requires a top-level commitment by management to:

- Enforcing vendor performance to the enterprise's information risk standards
- Knowing the business owner of each vendor relationship

- Reporting vendor risk performance periodically to each business owner
- And, holding each vendor accountable to meeting performance requirements

Achieving good third-party risk outcomes also requires that the business support an escalation path through which the business owner will escalate unmitigated issues within their vendor portfolio for remediation. We have seen organizations very successfully operate a formal vendor risk escalation program in which poorly performing vendors are placed on a 'watch list' and eventually placed on a 'do not do business with' list to motivate vendors to manage risk properly.

The two essential keys on which all third-party risk outcomes depend are strong business support and assignment of a business owner to each vendor relationship. From this foundation the vendor risk management program can flourish; without this foundation, efforts will likely be futile.

Third Deadly Sin: Not measuring and reporting risk and risk outcomes

According to RiskRecon's 2017 study of enterprise third-party risk management practices, 60% of programs reported program activities, while only 37% reported risk outcomes. Looking at the inverse of those metrics, 40% of third-party risk programs report no metrics and 63% do not report risk outcomes!

This is stunning – third-party risk programs exist to manage third-party risk and yet the large majority do not report their risk outcomes. That is like a for-profit business not reporting its financial results to investors. Without reporting risk outcomes, third-party risk management, at best, will be a regulatory-required checkbox. At worst, third-party risk management will be defunded completely. And why not? The program never demonstrated value in reducing risk.

Reporting both program activity and metrics is essential to third-party risk management success. Program activity metrics serve to inform the business of the degree to which you are managing the third-party portfolio. Risk metrics inform the business of the degrees and types of inherent and residual risks in its third-party portfolio.

Some metrics we've observed programs reporting include:

- The percent of vendors assessed for inherent risk
- Distribution of vendors by inherent risk tier
- The categories and magnitudes of inherent risk for dimensions such as sensitive data risk, transaction risk, reputational risk, and operational risk
- The percent of vendors for which control reviews have been conducted per program specifications. This serves to inform the business if the program is fulfilling its obligations as dictated by the risk policy
- Response times to requests to risk assess vendors

- The distribution of vendor residual risk, informing the business of the vendors that are exposing the organization to an unaccepted level of risk. Some organizations communicate this with ratings such as 'Mature', 'Satisfactory', 'Developing', and 'Unsatisfactory'
- Number of third-party issues by severity and age

Perhaps most importantly, proper metrics encourage a culture of mindfulness in managing third-party risk, that impacts to third-parties may impact the business and that these risks must be managed. They also serve to drive action — escalation of issues, elimination of non-performing vendors, and, in some cases, formal acceptance of risk.

Fourth Deadly Sin: Failure to address information security in third-party contracts

Ignoring information security provisions in third-party contracts, including (1) the right to audit the third party; (2) defining any availability / resiliency requirements; (3) data breach notification; and (4) remediation requirements for addressing identified vulnerabilities, for example, leaves a company with no recourse in addressing third-party issues. Without right to audit, risk exposure cannot be assessed. Without remediation requirements, identified risks may not be addressed.

Using a Legal-approved, standardized information security appendix to the Master Service Agreement with third parties ensures the company has visibility into and recourse to require corrective actions to protect its clients, assets, and reputation. Even if you aren't actively managing the risk of vendors, put in contracts the risk requirements that you want. Doing so will contractually commit the vendor to some minimum set of performance requirements and will position you for the future opportunity to assess their performance.

Fifth Deadly Sin: Not knowing your vendors

There is a reason that the first principle of the NIST Cyber Security Framework is asset management — you can't manage what you don't understand. That applies equally as well to third-party risk. You can only manage the risk of vendors that you know. The more vendors you know, the more you can manage, the less risk you have.

If your third-party risk program is new, you must decide how to roll-out your program to the vendor population. If your program is well-established, you must ensure that you are covering all the cracks of the organization where vendors may slip through.

For new vendor risk programs, discover and initiate management of vendors in a staged approach, rather than attempting to identify them all at once. Considering starting with covering new vendors, and then expand coverage to existing vendors through the contract renewal process. This approach provides two primary benefits. First, it gives you a natural method for growing your program over time, rather than trying to swallow the entire vendor population at once. Second, new vendors are the most motivated to comply with your risk management process as they want to win your business.

Over a matter of a few years, by managing new vendors and existing vendors as their contracts renew, you will cover the vast majority of your vendors. Then comes the challenge of digging out vendors that have slipped through the established process. We've seen a couple of interesting approaches here to ferret out vendors from the corners of the organization.

One company we work with conducts a monthly reconciliation of the accounts payable database against their vendor risk management database. Any vendors identified as not in the risk management database are flagged for inherent risk review and treated accordingly.

Most importantly, don't hold off on managing third-party risk until you know all of your vendors – get going with the resources you have. Prove value in those that you manage, build the case for more resources, and repeat. Along the way, provide estimates to executive management about the population of vendors still unmanaged.

Sixth Deadly Sin: Trusting, but not verifying

In entering into discussions with the Russian government on nuclear disarmament, U.S President Ronald Regan adopted the Russian proverb of 'trust, but verify'. The principle of 'trust, but verify' is wise to apply in managing third-party cyber risk, particularly given that it is your risk and not the vendors.

Vendors most commonly pass questionnaire-based assessments with perfect marks. A company we work with closely recently reviewed the questionnaire responses from 100 vendors. Nearly every vendor answered each question in the affirmative, representing proper deployment and operation of required security controls. Are these positive attestations sufficient to conclude that your risk is mitigated? Are all vendors really that good? Very likely not.

Vendor attestations of cyber risk management provide an understanding of the investments third parties have made in people, process, and technology to achieve good risk outcomes. However, attestations do not tell you how well they implement and operate their risk management program.

For example, a third party might respond positively to vulnerability management questions stating that they vulnerability scan their entire environment daily using a vulnerability scanning tool such as Qualys; that they subscribe to software security notices, and that their information security policy states a reasonable frequency for remediating vulnerabilities based on severity. However, objective data provided by RiskRecon might reveal that 20% of the third party's internet-facing software is unpatched and that a significant portion of the issues are critical and impact high-value assets.

Good risk management requires accurately and fully understanding risk. Vendor attestation of security helps you understand the investments they have made to achieve good risk outcomes, but that is only half of the information needed. Objective data helps you understand how well they implement and operate their program.

Seventh Deadly Sin: Limiting vendor risk management to periodic assessments

Managing vendor cyber risk through periodic assessments is insufficient. A lot can happen between assessments, even if they are conducted annually. Vendor data breaches could unknowingly compromise your data, risking penalties from regulators due to delayed customer breach notification. Critical vulnerabilities in vendor environments could go unaddressed, exposing your dependent operations and data to compromise.

Innovative organizations have pioneered the use of continuous monitoring to efficiently maintain awareness of their third-party cyber risk exposure. The continuous monitoring capabilities provided by RiskRecon enable them to easily detect and investigate material degradations in vendor cyber risk posture in a timely manner. RiskRecon customers have invented additional uses of RiskRecon capabilities to better manage third-party risk. These include:

- Dangerous Condition Hunting – Companies leverage the search capabilities of RiskRecon to periodically report and act on vendors that are operating software that is highly vulnerable to compromise, such as ancient versions of IIS, WordPress, and JBoss
- Critical Vulnerability Triage – Leverage RiskRecon to quickly identify which vendors and vendor systems are exposed to critical vulnerabilities, such as Apache Struts
- Monitoring Vendors for Data Breach – Proactively hunting for breach notifications for hundreds of vendors can be unmanageable. RiskRecon alerts customers to vendor breaches

Leveraging continuous assessment capabilities, such as those provided by RiskRecon, enable you to maintain cyber risk management of your vendors continuously, filling the gap between periodic assessments.

Disclaimer

The material furnished in this document is believed to be accurate and reliable. However, no responsibility is assumed by RiskRecon, Inc. for the use of this document or any material included herein. RiskRecon, Inc. reserves the right to make changes to this document or any material included herein at any time and without notice. © RiskRecon, Inc. 2018. All rights reserved.

About RiskRecon

RiskRecon is the only continuous vendor monitoring solution that delivers risk-prioritized action plans custom-tuned to match your risk priorities, providing the world's easiest path to understanding and acting on third-party cyber risk. Partner with RiskRecon to build your scalable, third-party risk management program and realize dramatically better risk outcomes. To learn more about RiskRecon's approach, request a demo or visit the website at riskrecon.com.

How to Get in Touch

- Call us at **(801) 758-0560**
- Email us at **sales@riskrecon.com**
- Visit us on the web at **riskrecon.com**
- Request a demo at **https://www.riskrecon.com/contact-us-demo.html**