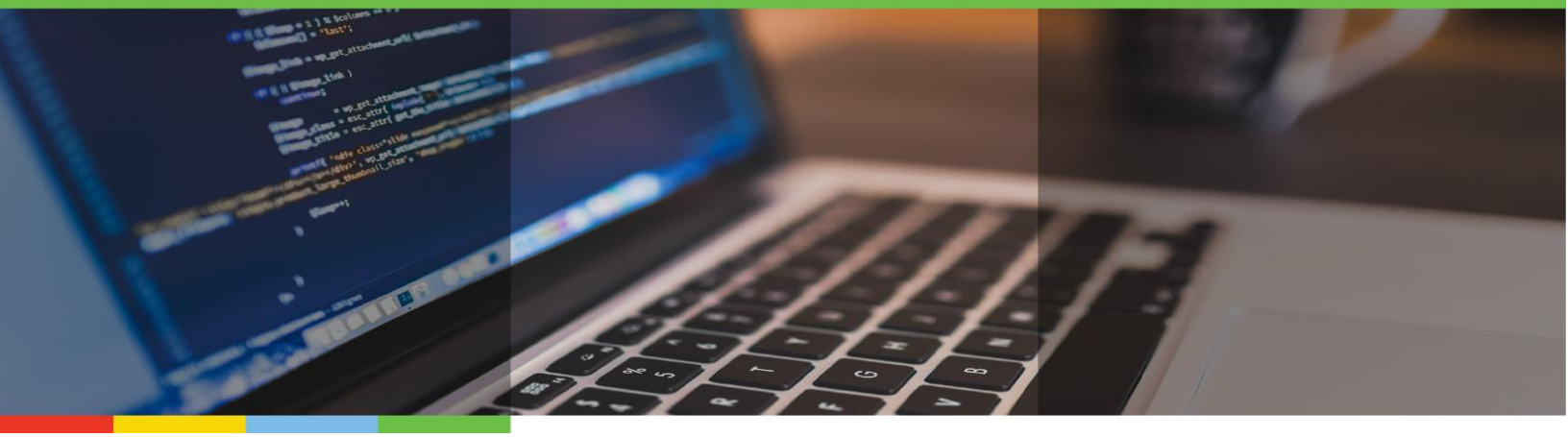

# MAKING THE BUSINESS CASE FOR RISKRECON'S VENDOR SECURITY ASSESSMENT AND MONITORING SOLUTION

Use Cases and Benefits Achieved by Incorporating
RiskRecon into Your Third-Party Risk Program

Last Revised: May 2017

riskrecon™
Control Your **Third Party** Risk Reality

## Document Objective

The purpose of this document is threefold:

1. Identify the various ways that your organization may benefit by implementing RiskRecon solutions.

2. Describe best practices for integrating RiskRecon solutions into your process to achieve these positive results.

3. Identify positive impacts on the effectiveness and productivity of your risk program.

Clients use terms such as "business case," "ROI" (return on investment), and "business justification" to describe these benefits.

## Document Organization

This document breaks down the business case into a set of use cases. This structure enables you to easily identify those applicable to the ways your organization intends to use our solution.

## Overview

RiskRecon's SaaS solution delivers transparent security measurements, analytics, and analyst-level insight to dramatically improve your third-party risk management program. By continuously monitoring an organization's internet presence, we deliver accurate, actionable measurements to reveal each vendor's "risk reality."

Our solutions do not replace, but rather supplement assessment processes that were designed for a very different IT environment when large sophisticated vendors provided most of your critical systems and you deployed them on your own managed networks. These processes for managing control effectiveness have changed little in the past 10 years, relying primarily on vendor surveys, questionnaires, and document reviews.

This "traditional" process is episodic, taking place often no more than once a year, and reliant primarily on manual tasks and simple tools such as spreadsheets and email.

By integrating RiskRecon solutions into your risk management processes, you benefit from highly accurate, continuous and actionable control effectiveness measurements. RiskRecon provides you with not only a more streamlined and effective control process, but also enables you to allocate resources in a more targeted fashion.

## Use Cases

The remainder of this document will describe what results to expect (and how to achieve them) by implementing RiskRecon and incorporating our solutions into your existing risk management processes. We explore five primary use cases:

1. Third-Party Monitoring
2. Pre-Contract Vendor Assessment
3. Fourth-Party Risk Measurement
4. Investment Due Diligence (mergers & acquisitions, etc.)
5. "Own Enterprise" Benchmarking

## 1. Third-Party Monitoring

Most organizations today rely on tens, hundreds, or tens of thousands of third parties—vendors, suppliers, outsourcers, and contractors. Many of these third parties have formal contractual relationships and security obligations, while others do not. Moreover, many of these third parties rely on their own third parties (i.e., fourth parties to you) to provide critical software, hosting, and infrastructure services.

To assess IT and security practices, your organization likely relies on a mixture of questionnaires, surveys, documentation, audited certifications, and on-site visits.

### *Where does RiskRecon fit in this process?*

RiskRecon provides valuable information and collaborative capabilities throughout this process:

- *Annual Assessment Planning.* Clients report that an analyst may spend up to two weeks preparing for the annual assessment of a critical vendor. This preparation involves gathering and reviewing prior year's attestation information and public database searches for any recent material changes. These searches often only identify major, publicly reported issues affecting the vendor—breach, financial distress, etc.

  With RiskRecon, analysts can review a full IT and security assessment in an instant. And this assessment contains significantly more depth and breadth than database searches alone. Thus, RiskRecon can shorten the prep process and provide unique insight to help analysts pinpoint areas for discussion with the target vendor.

  In time, rather than apply a single, generic process to all vendors, analysts can tailor where they do (and do not) spend time gathering additional information. RiskRecon clients report shrinking analyst prep time from two weeks to two days, while working towards a goal of two hours.

- *Attestation Verification.* Our clients today have little means by which to verify the information provided by their vendor in the questionnaire and document gathering steps. You may obtain audited certifications but those

are only a small window into an organization's security performance. And you may (or have a consultant) perform on-site assessments. However, these on-site assessments simply verify the documentation and written procedures are in place while doing little to verify how consistently and rigorously the procedures are actually followed.

With RiskRecon's objective measurements, you identify how well each third party conforms to their own documented practices. For example, if the organization provides assurances related to software patching and vulnerability management, but RiskRecon identifies a larger percentage of unpatched or end-of-life software, you can request follow-ups and clarifications.

Moreover, RiskRecon's continuous collaboration features enable you to share all results directly with the third party—no more manual spreadsheets or log emails without audit trails. Simply invite the third party to review their report and we will create log-in credentials directly into our portal. Coming later in 2017, you will also be able to assign tasks, designate priority status, and view vendor comments and remediation status.

For the first time you can compare verified, objective information against vendor attestation. While you cannot possibly manage every security practice for each vendor, our solution enables you to establish a base level of trust. And you can quickly determine security performance gaps that were not obvious from the attestation process or on-site visit.

- *Proactive Monitoring.* Before RiskRecon, organizations had limited means to monitor vendor security performance outside the regularly scheduled assessment period. Often little or no vendor due diligence is performed in between these annual periods.

  But as we all know, material changes in a company's security performance can occur at any time, often without warning or notification from the vendor. RiskRecon's automated solution operates continuously to track security performance changes both at overall ratings and granular criteria levels.

Our trending feature enables you to monitor historical performance at the overall rating and individual security criterial level. You can easily determine if a third party is consistently strong or weak, trending up or down, or simply erratic. This information allows you to tailor the frequency and scope of each supplier's assessment process.

In addition, with our alerting and reporting capabilities, you can build custom notifications triggered as soon as one of your third parties crosses a threshold in any security measure—software end of life, new threat intelligence, data encryption change, and so on.

With historical trending and alerting at your fingerprints, you can obtain more timely security performance information and adjust assessment scope to match each vendor's demonstrated performance.

- *Celebrity Vulnerabilities.* From time to time, a critical vulnerability emerges that causes regulators, executives, and the board to request immediate understanding of your exposure through your organization's supply chain. Today, you likely rely primarily on emails or phone calls to obtain this information from each vendor. This is a slow and unreliable process. Some vendors do not respond in timely manner and others not at all. Meanwhile, some third parties are not savvy enough to accurately determine if they are vulnerable, particularly if they rely on their own third parties (your fourth parties) for critical infrastructure.

  RiskRecon discovers and analyzes each third party's IT footprint without any reliance on stale or outdated databases. As a result, we enable you to quickly identify not simply which vendors, but which specific systems at each vendor are likely vulnerable to this new threat. And we provide faster and more accurate information without requiring you or the vendor to do anything.

## 2. Pre-Contract Vendor Assessment

How can RiskRecon assist in the pre-contract or RFP process? Our clients traditionally have a range of different approaches when incorporating security

information into their new vendor selection process. Many do not explicitly ask security questions, but may simply request that the vendor comply with the organization's standard security requirements. Others incorporate security questions into the RFP scoring process. Some clients do not address security until during the contract negotiation (after vendor selection), or after contract completion.

The lack of focus on security during the pre-contract process is understandable since a full security assessment of every potential vendor would impact line of business needs to move quickly and burden IT risk teams with a significantly increased workload.

However, with RiskRecon you can quickly obtain a security assessment of any potential third party. We can provide a one-time report (as opposed to continuous monitoring), and you can use the report in several ways:

- Use our numerical score as a factor in the RFP decision.
- Use our detailed data to pinpoint remediation actions required upon contract signing.
- Verify vendors meet their remediation deliverables committed to during contract negotiation process.

### 3. Fourth-Party Risk Measurement

As clients rapidly expand their use of SaaS providers and other outsourcers, they eventually learn that they have also entered relationships with many fourth parties. Specifically, many SaaS and outsourcers are too small or not skilled to manage the IT and security infrastructure to deliver their services. Increasingly, they turn to hosting companies, infrastructure providers, and the like.

Uncovering the systematic risks introduced by this expanding web of suppliers is quite difficult. It's challenging enough to measure control effectiveness of your third-party vendors and suppliers, let alone for the fourth parties who provide critical services to these vendors. However, without understanding these fourth-party risks you may not be able to effectively measure inherent and residual risks. Also, regulators and boards are growing more aware of these risk realities.

RiskRecon can help. One of our core capabilities is to identify a target organization's entire public-facing IT footprint—web, app, email, and DNS

systems. We do this for all systems registered and managed by the organization itself as well as all those assets that reside at a fourth party.

With this regularly updated footprint, you can quickly assess all fourth-party infrastructure providers, concentration of risk across your third parties, geographic locations used, and so on. The recent "Dyn failure" is a good example of a fourth party used by many third parties that had immediate impacts on the public websites of many companies, who had no idea Dyn was a critical part of their supply chain and service delivery. When Dyn was under attack, many websites were no longer available via domain name service resolution.

### 4. Investment Due Diligence

Our larger and more acquisitive clients often have a formal process or ad hoc team that evaluates potential investments in and full merger/acquisition with other entities. Currently, it is quite difficult to perform more than a cursory assessment of the target's IT and security practices.

In fact, it is often illegal or simply not feasible to have any direct contact with the target company. In other cases, your organization wishes to remain discreet, as it evaluates potential targets.

The same RiskRecon capabilities that provide risk assessments of your vendors and suppliers can also be directed to these due diligence activities. Our IT footprint and security assessment information supports the mergers, acquisitions, and corporate investment activities in several ways:

- Prioritize and more precisely value potential mergers and acquisitions based on potential security risks and program quality.
- Identify costs and potential issues with integrating/migrating systems by obtaining a comprehensive catalog of technology deployed.
- Substantially improve resource estimates for IT and security integration teams' post-investment close.

In summary, RiskRecon can provide precise information unavailable via other means to better value, prioritize, and budget for potential and closed financial transactions.

## 5. "Own Enterprise" Benchmarking

Many clients today rely on various off-the-shelf and custom-built tools for monitoring their own organization's security and vulnerabilities. Many of these tools are most effective when assigned to monitor a "known" or predetermined set of systems—net block range, URL address, etc. Other tools such as threat intelligence databases may cast a wider net for your brand but also have a large number of false positives that require follow-on analysis.

RiskRecon's "outside in" view of your own organization's attack surface area complements these existing solutions, by providing accurate and actionable measurements and often uncovering risks previously unknown to your company. Because our solution requires no foreknowledge of a target's IP ranges, net blocks, or URLs, we can automatically discover shadow IT, fourth-party hosted systems, and orphans/forgotten IT assets. And, once we discover them, we can perform our full security assessment and continue to monitor your environment for any new systems that appear in future.

Furthermore, because our solution is entirely passive/non-invasive and continuous, we can provide near penetration test quality results on a regular basis. We do not require lengthy test plans, coordination with outside testing companies, or other resource-intensive support. You can easily obtain regular assessments of your attack surface area from a bad actor's point of view.

Lastly, because our solution can evaluate any organization, you can benchmark yourself against any peer or competitor. We provide a normalized data set that facilitates comparing yourself with any other company using specific, well-understood security standards. Thus, we enable you to easily provide benchmark reports to your board, executives, and other key stakeholders. It is a common request by management to explain how their organization performs on absolute basis but also when compared to industry benchmarks, peers, and competitors.

## What if Your Third-Party Risk Program Is Just Getting Started?

Some clients do not have an established third-party risk management program or are seeking to redefine it. In these cases, often a missing component in the design process is a full understanding of the scope of the risk and security gaps within your supply chain.

Without this knowledge, it's difficult to appropriately develop the structure, depth, and resource requirements to support your new program. Similarly, you may lack the information required to build your internal business case to justify modernizing your program.

RiskRecon's solutions can help with this design phase. Imagine if you could obtain an objective portfolio-level assessment of your existing vendor's security practices. With this information, you would be able to quantify the performance of each vendor type, identify patterns, and determine overall gaps in your supply chain's security practices. You could also produce summary reports to better describe the scope of your organization's challenge, better design your planned program, and build a business case for management.

With RiskRecon's automated assessment capabilities, you can quickly establish the baseline for your existing third-parties' security performance and identify areas for further focus.

## Summary

RiskRecon provides unique capabilities to help you delivers dramatic improvements to your third-party risk program. Benefits include:

1. **Gain objective insight into third-party security performance and IT landscape.**
   - Deep IT asset discovery spanning third and fourth parties.
   - Detailed asset profiling—systems, software, hosting providers, and geo-locations.
   - Security control performance across 40+ criteria spanning 10 domains.

2. **Allocate risk resources to where they are needed most—high value, low performers.**
   - Vendor performance ratings.
   - Historical trends.
   - Customizable alerting.
   - Industry and peer benchmarking.

3. **Engage vendors with accurate, actionable security performance insights and corrective actions.**
   - Focus assessments on areas of weakness.
   - Rapidly identify and address current security issues.
   - Facilitate effective root cause analysis.

4. **Continuously monitor vendor security performance.**
   - Monitor security performance trends.
   - Alert on changes in security performance.
   - Automatically track issue resolution.

5. **Empower your vendors with RiskRecon analytics. Give your vendors continuous access to their own RiskRecon portal—no additional fees, no time limits.**
   - Accelerate vendor-driven issue identification and resolution.
   - Streamline vendor collaboration and data sharing process.
   - Enforce fair, fact-based vendor performance expectations.