Fortune 500 Financial Institution Reduces Cybersecurity Risk with RiskRecon

CASE STUDY

Financial Services

Customer
Fortune 500 company

Industry
Financial Services

Summary
Needed to advance cyber third-party risk management program to gain better continuous visibility into the most high-risk, business-critical vendors.

Results

- Over $600K in annual savings via cost reduction across people, process and technology
- Lowered annual Total Cost of Ownership (TCO)
- 35% productivity increase across the third-party program
- 35% more organizations annually assessed
- Fully operationalized implementation in three weeks
- 50% reduction in risk

THE CUSTOMER

A Fortune 500 company in the finance sector, this customer does business with thousands of vendors in a rapid, high-volume transaction-based global environment. As such, the firm was already running a highly mature third-party risk management program — but with an inferior third-party risk management and ratings solution.

Supported by an experienced 15-person team of risk professionals and established policies around vendor risk thresholds, the program was modeled to align with the NIST Cybersecurity Framework (CSF). The program's foundation was built on the following fundamentals: program management, assessment principles, and risk remediation.

However, the team found its performance improvements were plateauing due to technical challenges that were making it hard to prioritize their work with the incumbent solution. They were struggling to achieve accuracy and a continuous view of the risk posture for their vendors who represented the highest risk to their business, but who was also essential to operating the business.

> *"We needed continuous visibility into our high-risk vendors .... we have no margin for error in assessing the cyber health of vendors due to our fast-paced environment, sensitive data handling / sharing and vendor dependencies."*
>
> ***— Vice President, Vendor Cybersecurity Assessments***

THE NEED FOR HIGH-RISK VENDOR VISIBILITY MONITORING

The customer's well-established cyber third-party risk management program depended upon a monitoring tool that was delivering an unacceptable level of false positives about vulnerabilities and policy exceptions within its vendor environments.

More detrimentally, the previous solution was not able to provide contextual risk data or prioritization of mitigation actions based on the value of the vendor asset to the customer. Rather than being able to quickly understand the risk posture of a particular vendor, the team was forced to log more hours validating false positives.

As the customer started to see the volume of its outsourced vendors increasing rapidly, reaching a total of 350 high-risk vendors, the third-party risk team was being overrun with alerts on policy exceptions from vendors across the monitored portfolio. The obvious limitations in the platform made it difficult to hone in on what needed to be the top priority focus for action, namely helping to mitigate emerging problems in the most high-risk and highly critical vendor environments.

As the customer explained, the reason its team would even be collaborating with high-risk vendors versus just terminating a relationship was simple — high-risk vendors are usually essential to business operations. The expectation was that a cybersecurity risk ratings solution would become the force multiplier for an accurate, rapid assessment, which was not the case.

A higher risk tolerance doesn't mean that the high-risk vendors don't have to conform to a certain level of internal security standards for the organization assessing them. While the thresholds are different than for slightly less critical vendors, those internal thresholds provide valuable indicators of potentially vulnerable conditions that should indicate elevated risk levels. Threats such as newly named zero-day vulnerabilities present themselves in these highly critical vendor environments, that's when the team most needs this level of visibility to take action.

KEY REQUIREMENTS TO ENHANCE PROGRAM FUNCTIONALITY

The inability to track the real-time security posture within the most highly critical vendor environments with its current solution prevented the team from being able to produce alerts internally or to its vendors to manage vendor risk.

The need for end-to-end automation that's applied from assessment all the way through prioritized remediation was a necessary component for the team in order to save time and eliminate false positives. Further, the team wanted these capabilities in a platform that could show results quickly without a lot of tuning, which had always been a problem with the incumbent solution.

Furthermore, as the team was seeking to take its program to the next level, they had no tolerance for a lengthy tuning process. Part of this requirement was for the new solution to seamlessly integrate into their overall governance, risk, and compliance (GRC) model to ensure the workflow didn't have to change based on the new solution selected. The goal for them was to ensure that cyber third-party risk activities weren't siloed away from other risk management functions.

THE ONLY VIABLE SOLUTION: RISKRECON

This financial services giant replaced its existing solution with RiskRecon. By an order of magnitude, the transition to the RiskRecon platform produced an immediate set of positive business outcomes. The move to RiskRecon was seamless, spurred by RiskRecon's stellar support team to help the customer fully operationalize its new implementation in less than three weeks to enable the continuous monitoring of its 350 high-risk vendors.

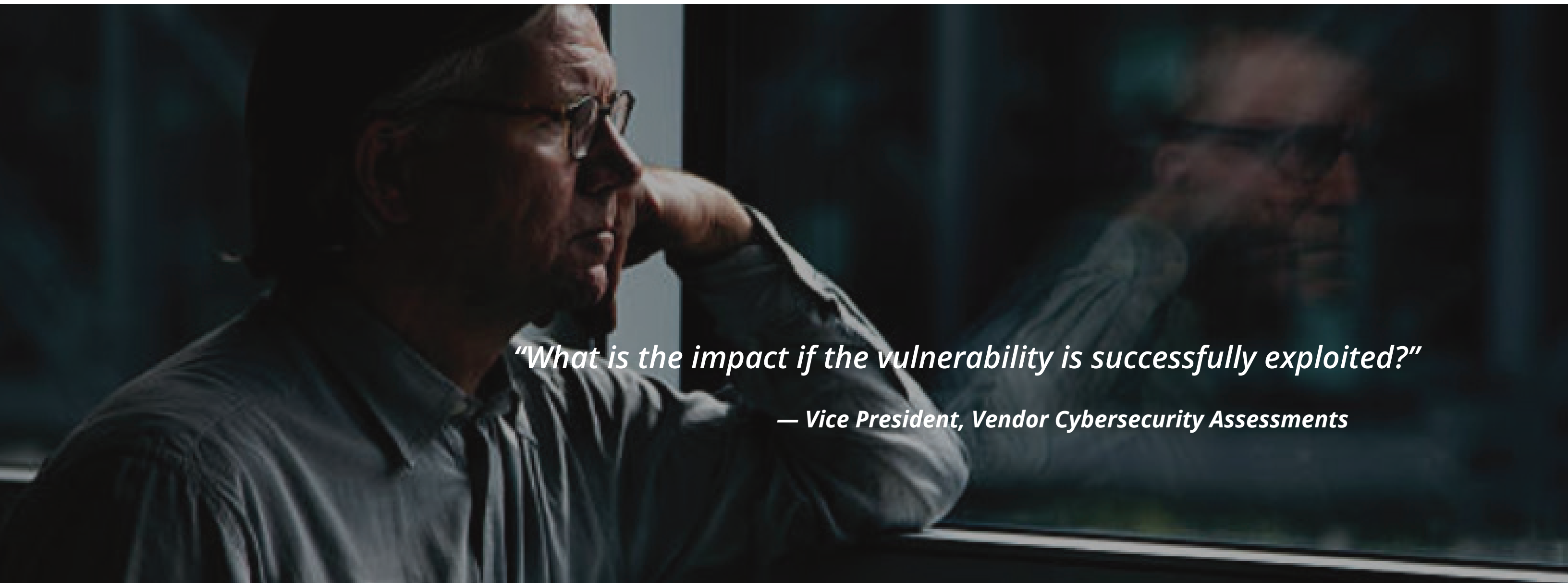
RiskRecon helped the client dial in its program with the most accurate risk data (independently validated at 98.5% accuracy[1]) on the market for the various dimensions of its vendors' risk postures.

Most importantly, the program was able to use the RiskRecon platform to custom-tune its risk thresholds and policies easily, and then move to prioritize the riskiest shifts in scoring by looking at the real-time changes occurring in the environments of its 350 high-risk vendors.

RiskRecon provided a reliable way to validate alerts, run a scan, investigate, and then fix the findings presented, all in a risk-prioritized format that automated the presentation of the findings to fix with a high degree of certainty. The high-fidelity analytics and workflow superseded the expectations of the entire team, delivering an experience that provided unprecedented velocity in time-to-result.

One example of the risk management benefits in play occurred when RiskRecon was able to help the customer prioritize its action when the Apache Struts 2 REST vulnerability was announced. By utilizing RiskRecon's discovery capability, the firm's team was able to easily discover potentially exploitable conditions in vendor environments and quickly determine if and how this vulnerability targeted the highly critical vendors within its portfolio. This could then be used to take the quickest action to help vendors mitigate the most valuable and vulnerable systems.

[1] Stratum Security, Report of Findings Regarding the False-positive of the RiskRecon Platform, July 3, 2019. https://www.riskrecon.com/data-accuracy-certification



"What is the impact if the vulnerability is successfully exploited?"

— Vice President, Vendor Cybersecurity Assessments

PROGRAM PERFORMANCE METRICS AND SAVINGS

The implementation of RiskRecon not only enabled this customer to scale its program efficiently, but it also saved the department $633,000 annually. These costs factor across people, processes, and technology associated with the third-party risk team. The dramatic cost-savings lowered the team's Total Cost of Ownership (TCO), delivering the value its incumbent vendor could not.

Equally important, the customer saw a 35% increase in productivity, allowing the team to monitor 35% more vendors annually. This was a breakthrough in what was already a highly advanced third-party risk management program.

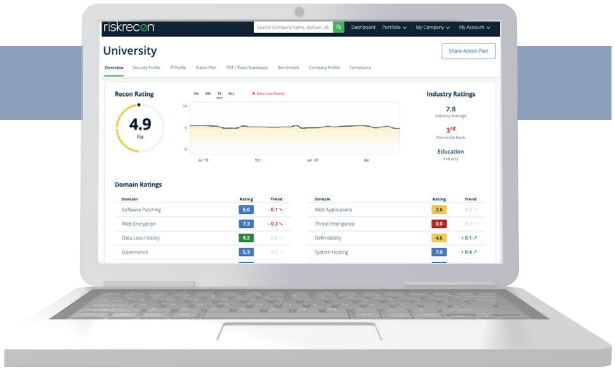
The added context and prioritization around asset value and the severity of the findings offered by RiskRecon made it easy to standardize and automate third-party risk-based assessments continuously. This resulted in the firm's improved ability to enforce remediation that was informed by accurate ratings and risk findings together.

The final metric, as reported by the customer's internal risk management function was the achievement of a 50% risk reduction — the optimal business outcome for any team responsible for managing cybersecurity risk.

Free Cyber Risk Report

Get a free cyber risk report that includes a summary of your organization's current cybersecurity posture with influencing risk factors.

Know Your Risk Now



University

Recon Rating: 4.9 Fix

Industry Ratings: 7.8 Industry Average; 3rd Percentile Rank; Education Industry

Domain Ratings

Domain	Rating	Trend	Domain	Rating	Trend
Software Patching	5.0	- 0.1 ↘	Web Applications	2.6	0.0 →
Web Encryption	7.3	- 0.3 ↘	Threat Intelligence	0.0	0.0 →
Data Loss History	9.2	0.0 →	Defensibility	4.6	+ 0.1 ↗
Governance	5.3	0.0 →	System Hosting	7.0	+ 0.4 ↗

riskrecon mastercard

www.riskrecon.com