Forrester Consulting Total Economic Impact™ Checklist Commissioned by Mastercard, April 2022

# How To Create Your Own Business Case For Enhancing A TPRM Program With Cybersecurity Risk Ratings

## A Seven-Step Checklist For Information Security Decision-Makers

According to Forrester Research, global security decision-makers that reported a cybersecurity breach within a 12-month span increased from 50% in 2019 to 63% in 2022.[1] This steady rise marks an uninterrupted business need to accurately assess cybersecurity risks and reconstruct public confidence and trust after a breach. In response, security firms continue to invent cutting-edge technology that refines detection rates, improves response times, and prevents the spread of detected malware. But as modern cyber defenses shift focus to proactively identifying and preventing cybersecurity threats within an organization even before a breach, businesses also have the opportunity and the responsibility to evolve their cyber risk management a step further and fortify their network of partnerships and vendors.

This checklist is designed to help readers develop a custom ROI assessment for a third-party risk management solution in seven steps.

## Implementing cybersecurity risk ratings improves risk posture and hygiene, and allows security teams to focus assessment efforts where it matters most.

Companies struggle to envision cybersecurity risk through a multidimensional lens that accurately captures the risk exposure of their organization, as well as third- and fourth-party partners. RiskRecon's continuous monitoring tool uses externally observable data to generate an aggregated rating of a firm's cybersecurity posture, enabling customers to reduce cybersecurity risk exposure, minimize audit efforts, and make data-informed decisions to mitigate risks that matter most to the organization.

RiskRecon maximizes efficiency with a tiered approach to cyberthreat identification that streamlines the third-party vendor selection process and extends visibility into fourth-party vulnerabilities. The tool provides insights into cyber issues to mitigate risk, customizes assessments to suit customer prioritizations, and improves attribution data accuracy.

## Summary of results from the Total Economic Impact™ Of Mastercard RiskRecon

### METHODOLOGY

RiskRecon, a Mastercard company, commissioned Forrester Consulting to conduct a Total Economic Impact™ (TEI) study and examine the potential ROI enterprises may realize by deploying RiskRecon.

To achieve these objectives, Forrester interviewed six decision-makers with experience using RiskRecon. The benefit frameworks presented have been simplified and condensed. For the full financial framework to estimate how Mastercard RiskRecon can impact your organization, please see the full study.



### ABOUT RISKRECON

RiskRecon, a Mastercard company, is a supply chain and enterprise cyber risk management tool that provides custom risk assessment and risk prioritization for its customers. RiskRecon equips business leaders across the finance, insurance, healthcare, energy, and defense industries to make third-party cyber risk decisions.

Here's how to quantify the impact these benefits could have on your organization:

## 1 Quantify automation-driven efficiency gains for analysts.

Understanding, acting, and resolving cybersecurity issues is becoming increasingly difficult to do effectively as the expanding ecosystem of third- and fourth-party partners far outpaces the growth of third-party risk management teams. These small but vital teams have historically relied heavily on manual processes, but to keep up with the changing threat landscape, automation is necessary.

RiskRecon improves productivity for analysts by up to 150% by offering a tiered approach to risk management, which empowers leaders to locate and remediate a vulnerability before it transforms into millions of dollars in cyber loss. Once the vendors are tiered based on cyber risk exposure and threat-level designation, your teams can focus on working directly with partners to resolve open weaknesses.

To calculate the business impact of improving your third-party risk management team's efficiency, use the following variables:

- Start with the number of employees responsible for handling security threats and vendor corrective action plans.
- Apply up to a 150% productivity lift on the team.
- Apply a burdened cost of a third-party risk management analyst (or appropriate role) to calculate the efficiency lift.

Further consider:

- How much time does the team spend manually entering data points into SharePoint or spreadsheets?

## 2 Calculate the increase in efficiency for routine third-party assessments.

While not intended to replace the vendor questionnaire process, better visibility and data-driven prioritization based on known risks increases assessment efficiency and reduces low-value efforts. RiskRecon empowers third-party risk teams with the ability to refine scope, tailor frequency, and validate third-party assessments. Greater transparency

> "The bottom-line justification for RiskRecon is it improves your risk governance. It improves your cyber risk assessment and, therefore, improves your ability to do better risk governance."
>
> **PARTNER, STRATEGIC RISK, PROFESSIONAL SERVICES**

enables targeted remediation efforts on vendors with the highest threat potential.

To calculate the value of routine third-party assessment efficiencies, use the following variables:

- In your current environment, how many vendor assessments are conducted annually?
- How much time does your team expend on across-the-board routine assessments of third-party vendors through assessment tools such as surveys? Using average hours per assessment, calculate how many hours are spent on assessments for new, key, and medium-risk vendors in your current environment. Assessment efforts likely vary by level of inherent vendor risk.
- Apply a 56% increase in assessment efficiency to calculate the number of hours of avoided assessment efforts.
- Apply a burdened cost of a third-party risk management analyst (or appropriate role) to calculate the efficiency lift.

Further consider:

- How responsive are the third- and fourth-party vendors to your assessments? How much time is consumed on follow-ups and necessary conversations?
- Is your team confident in the outcome of the assessments? Add in the time to inquire and research for accuracy.

> RiskRecon provides value to us for three reasons. First, it is a view into our own reporting, and it makes us aware of shadow IT. Second, it shows progress of the program because it is quantifiable data. And third, it gives us the ability to put a risk factor on our third-party program.
>
> **DIRECTOR OF INFORMATION SECURITY, HEALTHCARE**

## 3 Examine savings opportunities from leveraging RiskRecon data to avoid external audits.

Empowered with trustworthy data, analysts and decision-makers can identify third parties with persistently healthy risk ratings, reducing the need for a formal commissioned audit. Third parties with higher cyber risk exposures should continue to be subjected to more targeted audit efforts with RiskRecon data increasing the value of the audit by identifying concentrated risk exposure in specific areas of interest.

To quantify savings from avoided third-party audits, use the following variables:

- In your current environment, how many third parties are considered inherently high-risk?

- What is the current coverage ratio or number of inherently high-risk third parties undergoing audits?
- Apply 3% to calculate the number of audits avoided because the third party fell below the audit risk threshold as indicated by RiskRecon data.
- Apply the current expenditures per external risk audit to calculate savings.

Further consider:

- How are third-party vendors currently selected for audit? How many threats are identified and remediated because of the audits?

**4** **If your organization conducts M&A activities, evaluate the productivity savings from more efficient due diligence efforts.**

By using RiskRecon to gather information about a target's security program, your team can quickly identify major cybersecurity problems like obsolete infrastructure or poor patch management. Use this information to raise concerns around potential liabilities for decision-makers to consider as part of the deal. Reduce manual efforts for cybersecurity team while conducting due diligence.

To quantify savings from more efficient M&A due diligence, use the following variables:

- How many M&A targets are evaluated annually?
- Apply 80 hours of avoided risk team efforts per M&A event.
- Apply a burdened cost of a third-party risk management analyst (or appropriate role) to calculate the productivity savings.

Further consider:

- What has been the capital spending required to resolve infrastructure technology problems post-acquisition?
- The ability to identify problems may lead your organization to demand tail coverage to protect against cyber liabilities post-acquisition.
- Access to cybersecurity data may provide negotiation power for more favorable contractual terms.

> RiskRecon is the only tool where I actually trust the data. Point blank, period.
>
> **CYBER RISK MANAGEMENT AND GOVERNANCE MANAGER, PHARMACEUTICAL**

## 5 Estimate the value of business damage if a breach were to occur.

The damages a cybersecurity breach causes are hard to measure unless your organization has been subject to one. Rely on benchmarks and publicly available records to estimate the impact on your organization. According to Forrester Consulting's Q4 2020 Cost Of A Security Breach survey, organizations were likely to see multiple breaches per year with damages in the seven figures for larger enterprises.[2] RiskRecon customers noted that avoiding even one breach event enables an organization to break even on their RiskRecon subscription, and avoiding two breach events renders a positive return.

To estimate avoided breach costs, use the following variables:

- Using publicly available information, review what costs peers incurred after a breach.
- Estimate how many cyber breach incidents may result from an unidentified threat. What is the dollar amount cost of each incident? Include remediation and PR efforts.
- Part of cleaning up the mess of a cyber loss is rebuilding public trust and managing reputational risks. What is the cost to your brand, including lost revenues, customer churn, and lost contracts?

## 6 Think about how to measure the success of your cybersecurity program.

If your cybersecurity team does its job well, you may find that justifying program efforts can prove challenging. RiskRecon empowers customers to proactively respond to incidents and measure KPIs to illustrate and prove impact. Customers reported resolving 70% of their third-party security risks within a year.

To measure the success of your cybersecurity program, use the following variables:

- Measure a baseline to compare against each year. Demonstrate the value of the cybersecurity program with KPIs, including your firm's self score, ecosystem score, the number of vulnerabilities identified, the number of vulnerabilities remedied, the extent of shadow IT identified, the number of shadow IT vulnerabilities remedied, and the number of third and fourth parties monitored.
- Also document the continued improvements made to risk policies to correlate with reductions in risk.

Forrester developed a composite organization based on data gathered from customer interviews to reflect the Total Economic Impact that Mastercard RiskRecon could have on an organization and concluded that RiskRecon has the following three-year financial impact.

ROI

147%

BENEFITS PV

$2.4 million

NPV

$1.4 million

PAYBACK

<6 months

## 7 Evangelize your third-party risk program.

The importance of a third-party risk management program can be lost on non-IT business roles. Gain clarity for decision-making with the advantage of a simple scoring methodology to translate technical cybersecurity concepts into a common language for senior leaders in non-IT business roles. RiskRecon helps leaders make informed decisions about vendors, partnerships, and actions against cybersecurity threats.

---

[1] Source: "The Forrester Wave™: Cybersecurity Incident Response Services, Q1 2022," Forrester Research, Inc., March 28, 2022.
[2] Survey data represented is based on a data subset base of 84 manager level or higher security professionals at organizations within the 2,000 to 4,999 employee segment, taken from Forrester Consulting's Q4 2020 Cost of a Cybersecurity Survey.

To read the full results of this study, please refer to the Total Economic Impact™ study commissioned by RiskRecon.

**Project Director:** Veronica Iles