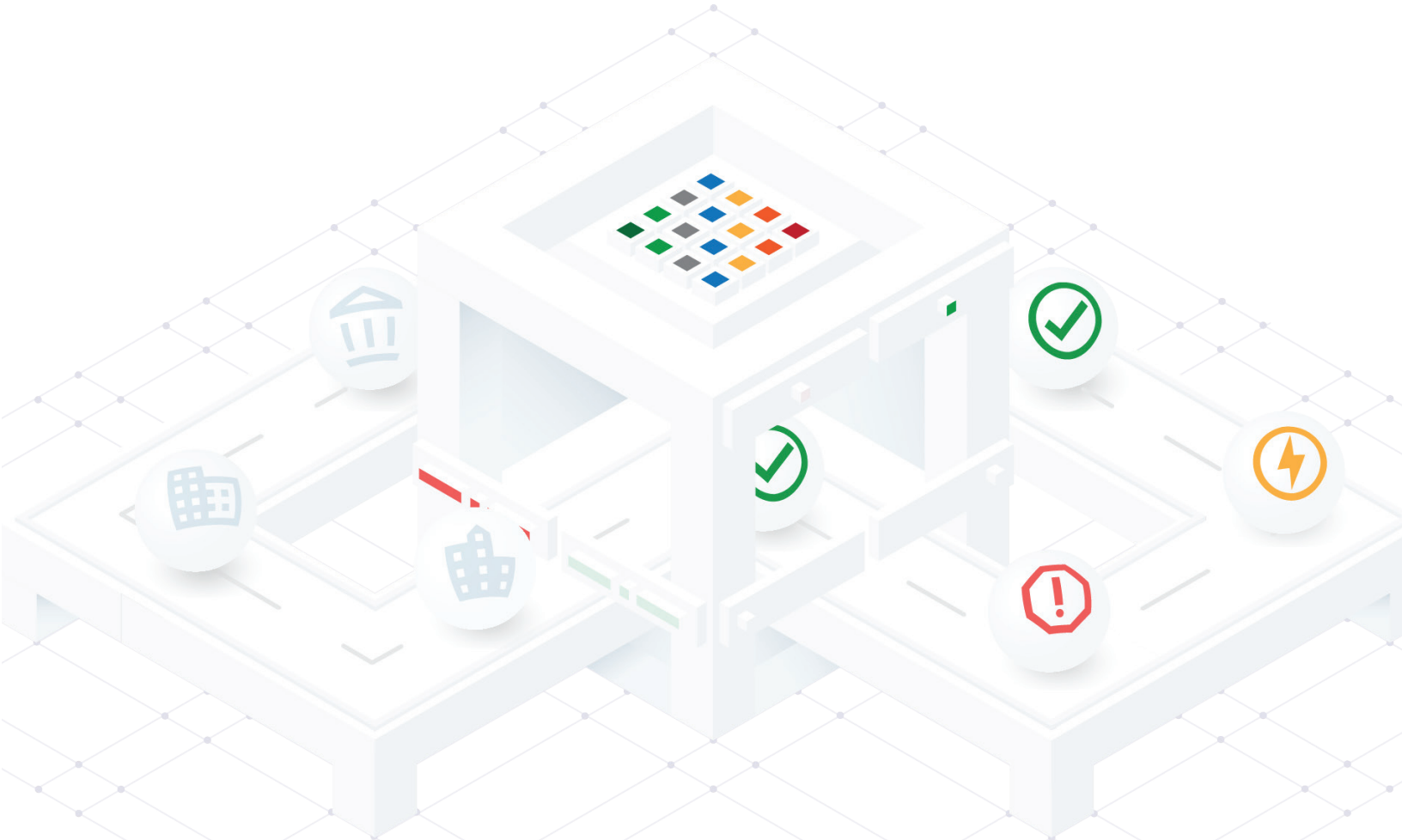
riskrecon

mastercard

Why Third-Party Risk Matters



RiskRecon.com
sales@riskrecon.com

Salt Lake City, UT
Boston, MA
(801) 758 - 0560

Table of Contents

Introduction

While many enterprises have taken tremendous strides in recent years to measure and manage the cyber risk present within their own IT systems, they struggle to extend that vigilance to third-party risk.

That's a problem in a time where third-party systems increasingly make up the backbone of modern IT. Enterprises today leverage cloud resources and technical connections with vendors and partners to go to market faster, meet customer demands, and stay competitive.

There's nothing intrinsically wrong with those third-party relationships, but they have the potential to come with a risky dark side.

After all, organizations entrust more of their crown jewels to third parties every day. They're sharing customer data with SaaS providers that help them with analytics, storing intellectual property on public cloud platforms, openly connecting their internal systems with the networks of technical partners. And the list goes on.

Each of these relationships has the potential to add considerable risk to the enterprise, because every third party that touches those crown jewels has the potential to compromise them.

As such, the more that enterprises build out their digital ecosystems, the more important it is for them to see and manage cyber risks incurred by their third-party relationships.

Third-Party Technical Relationships: More Present Than You Think

Many organizations realize that they need to do a better job at managing third-party risk, but they don't prioritize the problem because they don't realize the true scope of the risk.

Third-party technical relationships are rarely as isolated or limited as many executives seem to think. In fact, scratch deep enough under the surface of most modern IT architectures and you'll usually find that the most crucial infrastructure and processes rely heavily upon third-parties to bring the business full value.

That's because innovation in the era of digital transformation depends upon integrated systems and extended technical ecosystems. Third-party relationships are usually completely enmeshed in the way that organizations develop software and deliver digital services to external and internal customers. Some of the most common external resources found in the innovation supply chain include:

- Cloud platforms and hosting
- SaaS services
- Open API connections
- Third-party software components
- Specialized consulting services
- Data aggregation services
- Managed services

What's more, because digital transformation makes every business a software business, even seemingly non-technical business relationships often require the connection of IT systems and sharing of crucial data streams.

The point is that third-party connections are everywhere—and so are third party risks. Internal systems are rarely bubble-wrapped anymore. So even an organiza-tion completely confident in its own cybersecurity protections could be working with very little cyber assurance if it doesn't monitor and manage how its third- parties conduct their own risk management.

You Can't Abstract Away Risk

The fundamental truth about third-party risk is that an organization can abstract away IT complexity and outsource IT work, but it can never outsource the cyber risk.

When a third party breaches your customer data, the customer still comes to you for accountability. No matter who exposes the information, headlines still feature your company's name when your data is breached.

Multi-party cyber incidents that affect numerous organizations who have both direct and indirect connections to the initial victim are a troubling class of incident known as cyber ripple events. A recent study of ripple events shows that they can cause 13x the financial damage of a single-party incident.

Some dramatic recent examples that demonstrate the ripple dynamic in action include:

Computer Facilities

A third-party marketing firm working with Nedbank, one of South Africa's biggest financial institutions, recently exposed personal data of 1.7 million customers of the bank. Nedbank used Computer Facilities to run SMS and email marketing campaigns. A compromise of the third-party's systems led to exposure of all the data that Nedbank had shared with it.

AMCA

A breach of systems at American Medical Collection Agency (AMCA) compromised the personal information of over 24 million individuals. This single event at this third-party collection agency caused costly downstream impact at 29 different client companies who shared patient information with it. One of the most high- profile organizations was Quest Diagnostics. Approximately 11.9 million Quest patients were affected, and the firm now faces a class action lawsuit as a result.

Rocktop Partners

More than 24 million financial and banking documents related to mortgages originated by numerous institutions including Citibank, Wells Fargo, Capital One, and the Department of Housing and Urban Development were exposed by an unsecured cloud instance run by a small fintech startup Optics ML. The company had been tasked to run a cloud database for Ascension, a data and analytics company run by the parent company Rocktop Partners, which buys distressed loans and mortgages. The incident shows how third-party ripples can run in many concentric circles.

These are no isolated incidents. Cyber ripple events with downstream impact upon other organizations are demonstrably on the rise. Recent research shows they have been increasing 20% annually since 2008.

[1] https://www.itnewsafrica.com/2020/02/the-nedbank-data-breach-new-details-via-ceo/

[2] https://www.beckershospitalreview.com/cybersecurity/quest-diagnostics-hit-with-class-action-lawsuit-following-11-9-million-patient-data-breach.html

[3] https://www.housingwire.com/articles/47992-millions-of-sensitive-mortgage-documents-exposed-in-massive-data-breach/

[4] https://techcrunch.com/2019/01/23/financial-files/

The State of Third-Party Risk Management Today

Unfortunately, too many enterprises today are completely blindsided by down-stream impact from ripple events at their third parties. They never see the threat coming because they simply do not have the mechanisms in place to monitor how well their vendors and partners are managing risk in shared or connected systems.

According to Ponemon Institute, almost half of organizations do not earmark any of their cybersecurity budget to help its vendor risk program with third-party risk management. Most organizations remain relentlessly hyper focused on cyber-security internal controls, without looking to very relevant external systems.

Companies that do spend money to help with vendor risk only spend an average of about 17% of that security budget third-party risk management—and that money is often spent on ineffective remedies.

The truth is that many third-party risk management programs rest on account-ability mechanisms that were devised in a very different technology era. When the field of third-party risk management arose a couple decades ago, the standard for checking up on external parties was via vendor questionnaires, documentation, and the occasional visit to a larger third-party vendor's data center.

This worked okay when there were a relatively small number of vendors to be assessed, the company data was still resided on-site, and the vendors themselves had large, sophisticated security teams (e.g., Microsoft, Oracle, EMC, etc.).

Of course, this world no longer exists—but the third-party risk management process has not changed. As a result, many enterprises are flying blind with regard to third- party risk. They're sharing crown jewels without any assurance that moment-to- moment, day-in and day-out, ALL of their vendors are reliably protecting their risk interests.

The question is, how much of your business viability can you afford to rest on unverified trust? Do you trust:

- That your most critical vendors have a 10% internet system software patching failure?
- That all of your vendors consistently focus threat intelligence operations on internet points of presence that matter?
- That vulnerabilities in your vendors systems can't be exploited to attack systems where your data resides?

In cybersecurity it’s not good enough to simply trust.

No other area of security relies almost entirely on the “honor system” to manage risk. It would be like sending email to all employees, asking them a long list of security questions about their computer. And then entirely relying on their answers without any testing, monitoring, or verification.

You must verify third-party risk posture, too. Because if the vendor performs poorly as an enterprise, eventually that poor performance will show up in systems relevant to you.

Overcoming Visibility Gaps

Reliance on third-parties for collaborative innovation is a foregone conclusion to bring about digital transformation. But incurring undue risk from third-party relationships doesn’t have to be.

With the right tools at hand, organizations can effectively monitor and manage the risk posture of their third-party portfolio to bring it in line with that of internal systems. Third-party cyber risk management is ultimately about verifying trust in an enterprise’s entire digital landscape.

Where Do You Go From Here?

Cybersecurity Risk Ratings 2020 Market Outlook

Download your complimentary copy of this new report today to learn more about key trends and business cases you can expect over the next 12–24 months. This is a must-read for security and risk professionals.

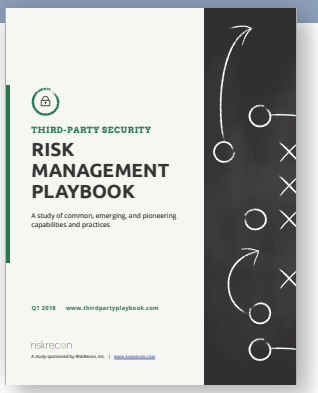
Download the Report

FORRESTER®

Third-Party Risk Management Playbook

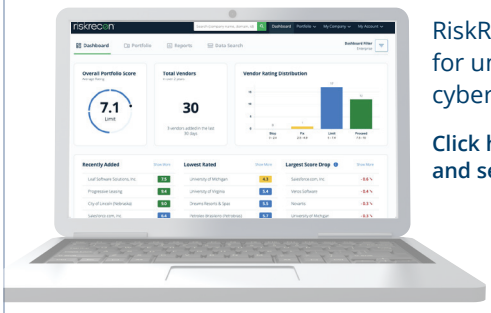
The Playbook is built directly from the third-party security practices observed in 30 leading enterprises around the world. Compare your own program with the Playbook data and identify the capabilities and practices that make sense for your organization.

Get the Playbook



See RiskRecon in Action

CTA TO COME



RiskRecon is the most effective solution for understanding and acting on third-party cyber risks.

Click here to learn more about our approach and see our platform in action.

See RiskRecon in Action