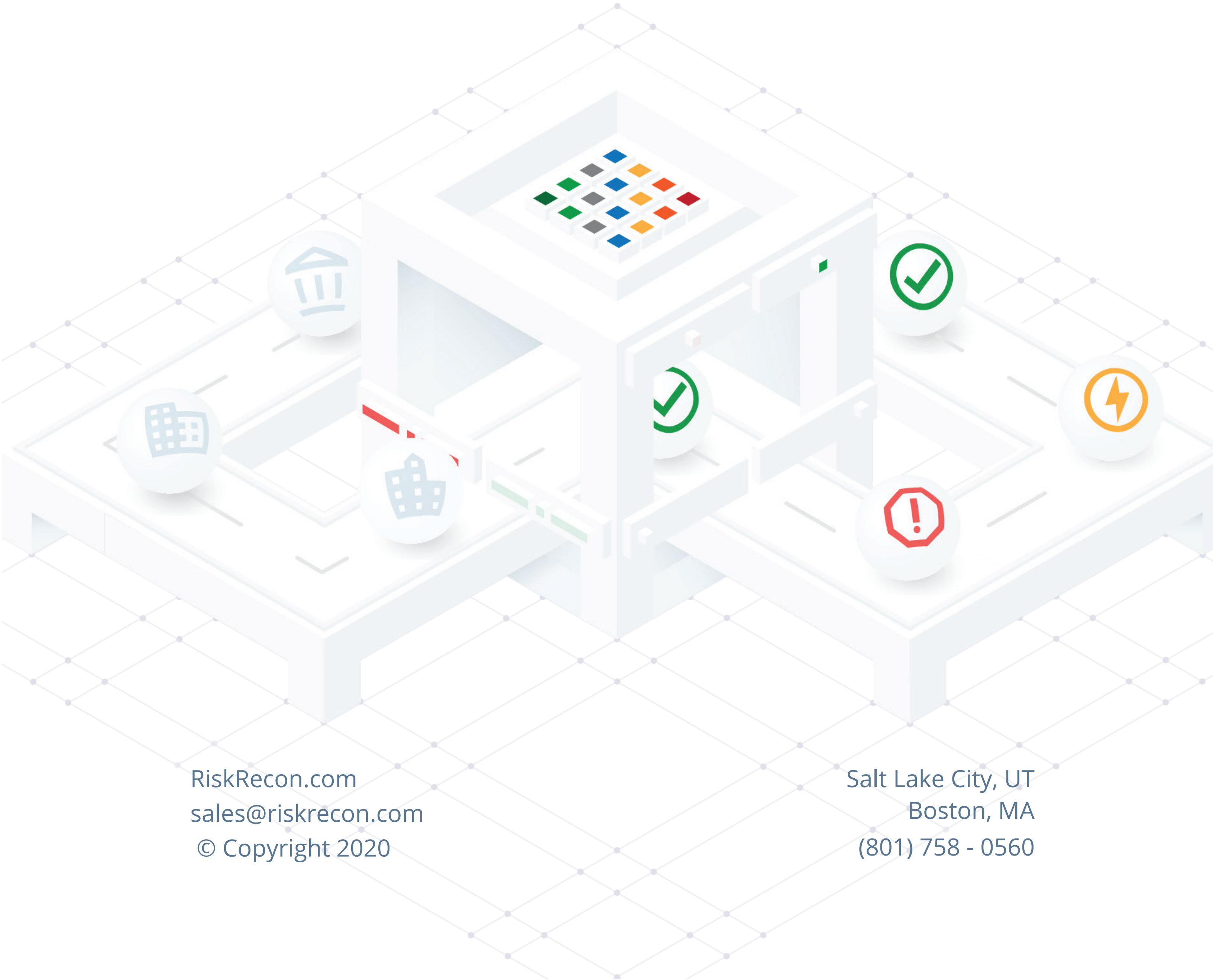
The Analyst View: State of Cybersecurity Risk Ratings

A Q&A with Forrester Senior Analsyt Paul McKay



RiskRecon.com
sales@riskrecon.com

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

Table of Contents

Why this Tech Matters and the Gaps it Fills

Cybersecurity risk ratings are rapidly becoming a critical component of third-party cyber risk management programs. Security leaders are beginning to use them to find quantitative data to scrutinize the statements made about security by their third parties, supporting business critical commercial discussions and risk decisions. Increasingly, security leaders are seeking to operationalize this data to build more robust information from which they can base their risk management decisions upon.

RiskRecon spoke to Forrester's London based Senior Analyst Paul McKay to discuss how security leaders are making use of ratings data within their third-party risk management processes.

RiskRecon: From your perspective Paul, as a risk practitioner-turned-analyst, what are the key gaps or blind spots that cybersecurity and risk management teams currently have in terms of managing cyber risk that sits outside their organization? What problem is this class of technology solving?

Paul McKay: There are several common gaps that I see within third-party risk management. In many organizations, a common stumbling block is to even be able to identify who all your third parties are. It is quite challenging to get your head around your third-party security risks if you are not able to undertake this foundational step.

It is also common to see difficulties in getting prioritization correct, leading to unnecessary efforts placed on suppliers who don't merit that attention and vice versa. Also, almost all the due diligence, whether this is a review of security questionnaires or on-site auditing, is performed at the beginning of a contract.

When we even get to the security questionnaires, the responses suffer from issues of bias, inaccurate data and bold statements professing how wonderful the vendor's security program is. Having objective data sources that are accurate and based on open data, is a challenge and we need to establish ways of doing this to counter the inherent positivity found in many third-party security questionnaires.

For example, I see a gap in continuous assessment during the life of a contract. Many programs are not continuously assessing the risk posed by critical third parties, so I see a big gap here that needs to have more attention paid to it.

It is not uncommon for good audits to surface several issues that never get addressed because nobody in the organization is pushing it hard. Without remediation, the entire process does not deliver the risk management benefit it is supposed to. Finally, given these challenges, it is not surprising that determining fourth parties (suppliers of your direct third-party providers) is a problem we have not been able to scratch the surface of yet.

RiskRecon: When it comes to the third-party risk management lifecycle, at what stage do you suggest the maximum focus and effort should be put into using cybersecurity risk ratings? How do you know you are ready and how do you extract value quickly?

Paul McKay: The two stages I think are most important to focus on are the prioritization effort and how you manage and drive remediation.

Taking prioritization first, this really does drive where you choose to place your focus, accepting that you won't have the financial or human resources to review every third-party supplier with the same level of depth. Getting this right is just as important as the process of doing the assessment (whether this involves questionnaires, ratings data, auditing).

The second part, which I think gets lost sometimes, is that a great audit report surfaces some crucial issues that need to be addressed. A lot of the time, the burning issues are fixed and then all the other issues go nowhere. I think the remediation aspect, linked to continuous improvement, is critical.

In my mind, not performing remediation kind makes me think, what is the point of all of this? If we do all this assessment work and do nothing with it, we just create a paper trail (digitally or physically) of great audits that never actually reduced any risks.

Operationalization and Value

RiskRecon: How does remediation differ when it comes to third-party cyber risk as opposed to any other IT risk environment?

Paul McKay: The concept of management control is critical here. Within your own IT risk environment, you can exert some control and direct influence to bring your weight as a security organization to bear to change things. You can commission projects and influence other parts of the business to change behaviors or spend time, money and resources undertaking projects to reduce risk.

In the third-party case, your only mechanisms are contractual. It is crucial to get embedded right from the off to perform audits and gain the cooperation of the third party in your security assurance efforts. Expect remediation to be discussed through the lens of contractual change controls and suppliers to challenge based on commercial priorities. This makes remediation more difficult and potentially more costly than it is for your internal environment.

However, suppliers don't want to be perceived as failing in their security obligations, they want to make it as good as they can because it helps them with not just you but all their other customers as well. I often find the quality of the personal relationships and level of trust obtained helps to build an easier path to remediation.

Where the relationship is positive and constructive, progress can often be made without having to look at what the contract says every five minutes. However, it becomes more combative when the relationship between the business and the supplier is poor and there is a low level of mutual trust.

RiskRecon: What are some of the emerging use cases in which cybersecurity risk ratings are starting to deliver value to security and risk teams?

Paul McKay: While third-party risk has been the most popular use case to date for this class of solutions, I see several emerging use cases that are becoming popular. I'd highlight first the emergence of the enterprise cyber risk management use case, using the ratings data to assess and manage your own performance and reputation. I see this being a clear focus for organizations that act as a service provider to others and see growing interest in its use in large global organizations with complex legal and business unit structures.

In these types of companies, it is not uncommon to see global security teams relying on self-assessment reports from business units' local security or IT teams. These suffer from the same quality issues as third-party questionnaires.

In addition, I see increasing interest in the investor community in using these ratings in a number of ways, particularly scrutinizing companies' cybersecurity posture during M&A and also when choosing whether to invest in a company or not.

This latter point may become a component of ethical investment frameworks, would it be considered acceptable for a company with a poor track record in cybersecurity to receive investment from certain mutual funds and investment houses? I think these and multiple other use cases are going to become more mainstream over the next few years.

Measurement and Reporting

RiskRecon: What information is typically shared with a board/executive team regarding third-party risks?

Paul McKay: At present, you are seeing information being shared that is very audit centric and more about counting audit issues of certain severity that come up via third-party risks. There is also likely to be a focus on a small number of high-risk suppliers that are crucial to the delivery of substantial components of overall business revenue. I am beginning to see some security executives use ratings to show the cyber posture of the supply chain more holistically to give a sense of the security capabilities of key third-party suppliers as well. This is earlier in its development, but boards like the simplicity of the concept and it has helped level the communication between technical security professionals and a non-technical business audience. I see this continuing in prominence in the coming years as a component of board-level communication about third-party risk issues.

RiskRecon: Could you describe some key measurements or results that an organization should look to reach when establishing a strong third-party risk management program?

Paul McKay: In my mind, the key measurement here is risk reduction achieved through driving remediation action with third parties. From a board perspective, this is but one data point in how they assess third-party risk. If the overall risk posture is reduced, because suppliers risk postures are getting lower, this helps. This can be measured by looking at something like a rating as one way of doing it, or qualitatively by tracking the reduction in the frequency and severity of security issues picked up from the third-party risk program. I think ultimately what the board wants to be assured of is that a third-party security risk materializing does not substantially impact the ability of the business to generate revenue and deliver its services to its customers.

RiskRecon: For security leaders seeking to use ratings data in their processes, how have you seen this done and what are some of the best practices for operationalizing this technology?

Paul McKay: Security leaders are presently looking at how they map not just the overall ratings but the detailed ratings data to controls. What they are looking to do is to see how the questionnaire responses, obtained from vendors, measures up to what the ratings data shows is really happening in their external footprint. So, if a vendor is saying it has a beautifully defined patching process, which is always up to date, but the ratings data shows that the external infrastructure is full of critical and high-risk vulnerabilities, then you know there is a consistency problem that you can investigate further. At present much of this effort is manual, so many security leaders are starting to explore integrations with existing GRC toolsets and other technology that they are using for their broader third-party risk management program.

Cybersecurity Risk Ratings 2020 Market Outlook

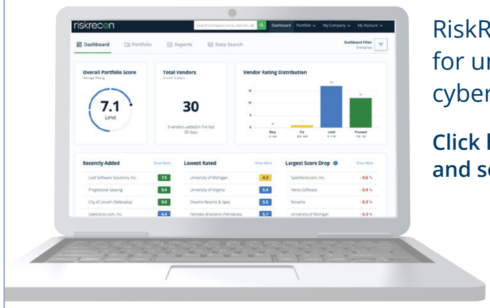
Download your complimentary copy of this new report today to learn more about key trends and business cases you can expect over the next 12–24 months. This is a must-read for security and risk professionals.

Download the Report

FORRESTER®

See RiskRecon in Action

CTA TO COME



Recently Added		Lowest Rated		Largest Score Drop	
Leaf Software Solutions, Inc.	7.5	University of Michigan	4.3	Salesforce.com, Inc.	- 0.6 ↘
Progressive Leasing	9.4	University of Virginia	5.4	Veros Software	- 0.4 ↘
City of Lincoln (Nebraska)	9.0	Dreams Resorts & Spas	5.5	Novartis	- 0.3 ↘
Salesforce.com, Inc.	6.4	Petroleo Brasileiro (Petrobras)	5.7	University of Michigan	- 0.3 ↘

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