

# Trends in Third-Party Risk Management

Q&A with Gartner and H-ISAC



**Third-party risk management has become a focus for most organizations** due to the rise in disruptive incidents caused by a vendor operating with poor security practices. Recently, RiskRecon founder Kelly White sat down with Sam Olyaei, Director at Gartner Research, and Errol Weiss, Chief Security Officer at Health-ISAC, to discuss their client's experiences regarding third-party risk management. These industry experts discuss current trends around all things TPRM and how to stay ahead of third-party risk.

---

**Kelly White, RiskRecon:** From what you are hearing, are some organizations doing a better job at managing third-party risk than others, or is every firm operating behind where they need to be when it comes to managing third-party risk?

**Sam Olyaei, Gartner:** We have a maturity assessment at Gartner that we call internally, "IT score for cyber security," and it looks at all the processes that we expect to see as part of a cybersecurity program and one of those processes is the third-party security process. That's the least mature process across all of them, in our database. On a scale of one to five, CMMI (Capability Maturity Model Integration), which is a typical scoring platform range that we use, third-party security is likely an average of about a 1.8 on that scale.

From my advisory interactions with clients, I've made a few observations. First, most organizations do not deal with third-party risk because they don't know who owns third-party risk in the organization, and they feel like they shouldn't themselves. Second, the people who do own or do manage third-party risk only do it from a vendor perspective, so they equate third-party security or third-party risk management with vendor risk management or vendor security, so they don't take into account suppliers, regulators, or customers. Third, those firms that manage third-party risk well are still only focused on the static side of third-party security, and what that means is the static assumptions of doing questionnaires, certifications, and audits tell us what has happened in the past, not what's going to happen in the future. It's not dynamic, it's not futuristic. It's not predictive analysis. It's prescriptive if you will. It's a point-in-time assessment.

**Errol Weiss, H-ISAC:** I was thinking about the answer to how well H-ISAC organizations are managing third-party risk, and my answer was going to be, it really depends on the overall maturity level of the information security program. I probably tend to agree with Sam's assessment from what I've seen so far, unfortunately. I think, and Sam also touched on this as well, I think that it is true that there is a lot of debate about who owns this, and I think CISOs probably would feel that they own the third-party information security risk. It is the right place to start, but pointing to the bigger picture here, I do think at some corporate-level function, there should be an owner of the third-party risk management function, and it would include things such as the fiscal risks, business risk associated with outsourcing and using those service providers, for example, in addition to the information security risks that come along with that.

## Is there a clear owner of third-party risk?

**Kelly White, RiskRecon:** Given the growing number of risk domains related to third parties, do you think there is going to be a call to reorganize within security/IT functions so that there is a clear owner of third-party risk?

**Sam Olyaei, Gartner:** I would argue the opposite. I would say there is no clear owner for a reason because those things touch on a variety of different aspects, when you think about just cyber risk in general, it's not just the information side, it's also the physical cyber side. It could also be the vendor side, so you need to bring in procurement, legal, and operational technology folks. I expect to see more distribution of roles across the organization to the point where cybersecurity becomes more of an oversight function, and essentially the business units themselves would be in charge of making decisions on cyber risk rather than cybersecurity making decisions on cyber risk, which is what many organizations have today.

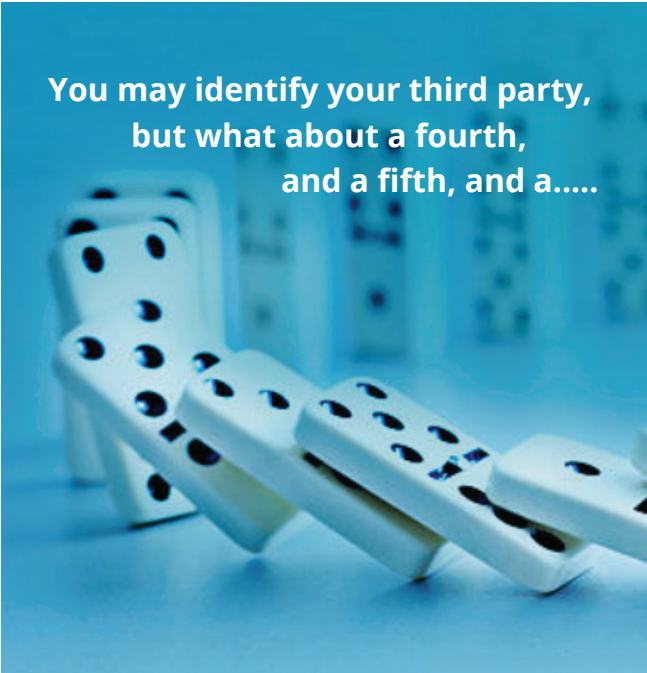
I would say what I see coming is not a re-organization, but a refocus. I've dealt with many cyber security leaders who basically not only have cybersecurity, but they own business continuity, privacy, IAM (identity and access management), third-party risk, and you can just keep adding on to that list. The reason they keep adding to that list is that nobody in the organization wants to take ownership of it. You end up with a situation where the security leader can't focus on one thing, they have to focus on a broader strategy on things that don't mesh well together.

Additionally, you realize that regulations are going to start to push for these things individually, taking privacy as an example, GDPR will deem that you need to designate a data protection officer, however, the data protection officer is not the same thing as a CSO, and you start to see things emerge from compliance mandates. I think third-party is still in that emerging phase, but we're going to get to a point where this becomes more of a holistic risk problem, but then ideally, there would be an enterprise risk management officer or an enterprise risk officer or a chief risk officer in charge of a lot of these sorts of risks at the bottom of the priority list.

**Kelly White, RiskRecon:** Given Gartner's assessment that third-party risk management is at a 1.8 on a one to five CMMI maturity scale, how much risk do you think organizations are taking on unnecessarily or avoidably because of that state?

**Sam Olyaei, Gartner:** The number tells us that the average third-party risk management process is not repeatable and scalable across the organization. It's not that there is a lack of a process, it's just that it's not scalable and repeatable across multiple entities. By default, when it's not scalable and repeatable across multiple entities, you are technically at a high level, and not actually doing a risk assessment on a lot of these entities and things that you have left. In reality, I would say the biggest issue with third-party risk is discovery, not identification, people don't know what they don't know.

You can use all sorts of services to identify what you might think are your third parties, but then there's always the fourth-party, there's always the fifth-party, there's always the supplier of that third-party, and so on. On top of that, business unit executives and leaders continue to go out and procure SaaS applications without involving the cyber security team. How do you identify those? I wouldn't say necessarily it's more risks, I would just say it's newer kinds of risks.



**You may identify your third party,  
but what about a fourth,  
and a fifth, and a.....**

**Kelly White, RiskRecon:** If you were to build a third-party cybersecurity risk management program from the ground up, what are the capabilities and functionality that are the highest priority in your mind?

**Errol Weiss, H-ISAC:** I think this also needs to live at a corporate enterprise level, because it does involve so many different parts of the organization to do it right, so it's not just a cyber problem. It would involve physical security, business owners, and leaders as part of that risk identification process. One of the other pieces I think is key in building a program is shared assessments methodologies. As the owner of third-party risk at this theoretical company, I do not have to necessarily foot the bill for every single one of the assessments that we're being asked to do, that I can leverage what's been done by others and use that as part of my overall risk management process.

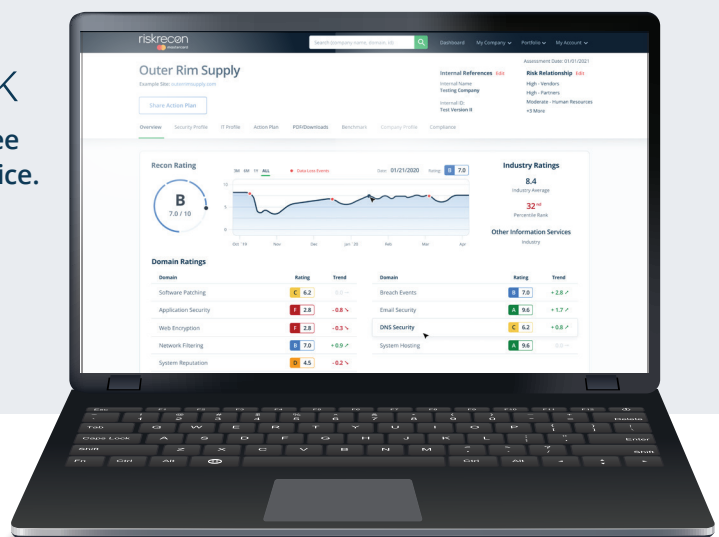
**Kelly White, RiskRecon:** Given the reality that people are still struggling just to manage the third-party risk, where are firms standing on identifying risks from n-th parties?

**Errol Weiss, H-ISAC:** I'm seeing activity in the healthcare area around Nth-party risk identification. Many firms are starting to use security rating services tools, like RiskRecon, to get an understanding of who they should be wary of based on if there is a data breach or an incident.

**Sam Olyaei, Gartner:** Nth-party is coming to a movie theater near you. I think most people don't even account for third-party, let alone, fourth, fifth, and so on. But I think the biggest problem today is the problem of discovery. Again, there are usually two mechanisms that we use to discover third-party risk. One is using an IP address and the other is using a domain. It's very hard to correlate an IP address or a domain of a fourth party to a fifth party to a sixth party. When you have a security rating tool you can identify the third parties that you are associating yourself with. The more you go out into the wild, the more these Nth parties will exist, and ultimately, this becomes a risk management conversation. Firms need to look at purchasing decisions. They need to look at cost decisions, they need to look at legal clauses and contractual clauses. Cybersecurity is only one part of that. Security ratings products allow the risk owner to say, "Listen, this company scored X on RiskRecon when we ran their scan." You have now started a conversation with that business executive because they were not aware of the intricacies of third-party, fourth-party, fifth-party, etc. That discovery is helpful, but to the point and can make a difference in terms of purchasing decisions or legal and contractual clauses.

Know Your Third-Party Risk  
Get free access to the RiskRecon portal and see the security ratings of up to 50 vendors of your choice.

Get Access Now



RiskRecon, a Mastercard Company, enables you to achieve better risk outcomes for your enterprise and your digital supply chain. RiskRecon's cybersecurity ratings and assessments make it easy for you to understand and act on your risks, delivering accurate, risk-prioritized action plans custom-tuned to match your risk priorities. Learn more about RiskRecon and request a demo at [www.riskrecon.com](https://www.riskrecon.com).



[www.riskrecon.com](https://www.riskrecon.com)

E: [sales@riskrecon.com](mailto:sales@riskrecon.com)

**Disclaimer:** The material furnished in this document is believed to be accurate and reliable. However, no responsibility is assumed by RiskRecon, Inc. for the use of this document or any material included herein. RiskRecon, Inc. reserves the right to make changes to this document or any material included herein at any time and without notice. © RiskRecon, Inc. 2018. All rights reserved.

© 2022 Copyright RiskRecon, a Mastercard Company