Cybersecurity Risk Ratings Market Outlook, 2020 And Beyond

CISO Trust And Transparency Issues Drive Market Consolidation And Exits

by Paul McKay

March 16, 2020

Why Read This Report

Cybersecurity risk ratings vendors leverage externally available data about a firm to rate its cybersecurity posture. These vendors have now become mainstream despite customers, suppliers, and investors either loving them or hating them. Security and risk professionals should read this report to find out the major trends to expect in this market in the next 12 to 24 months.

Key Takeaways

The Cybersecurity Risk Ratings Market Will Consolidate

Trust and transparency are core to vendors operating in the cybersecurity risk ratings market. But there is only so much of it to go around, just like the credit reference agency market from which vendors in this space take inspiration. Expect smaller ratings firms to exit the market or be acquired.

Firms That Lag In Building Operational Integrations Will Flail In The Wind

CISOs find these solutions useful in use cases such as enterprise cyber risk management and supply chain management. Vendors that fail to realize that ratings are part of a wider business process will struggle to maintain relevance to security leaders.

Cybersecurity Risk Ratings Market Outlook, 2020 And Beyond

CISO Trust And Transparency Issues Drive Market Consolidation And Exits

by Paul McKay
with Joseph Blankenship, Melissa Bongarzone, and Peggy Dostie
March 16, 2020

CISOs Want Operational Insight, Not More Noise

Cybersecurity ratings vendors are the Marmite of the cybersecurity space.[1] Security leaders we speak to report either being heavy users or heavy detractors of this product category. Supporters of ratings solutions like the simplicity of the output and it to be a useful tool for communicating with the board. Detractors complain of opaque ratings algorithms, inaccuracy, and attribution issues of correctly mapping assets back to companies. Security leaders we spoke to struggled with using the data in their existing operational workflows such as third-party risk management and internal security risk management. Ratings vendors are responding by building integrations into other CISO workflows such as third-party risk management and enterprise risk management processes. Vendors are also making the data useful rather than have it become another noisy signal.

The Industry Will Consolidate And Focus On Providing Operational Insight

Mastercard's acquisition of RiskRecon in early 2020 created a lot of market buzz.[2] The entry of a credit card company into this market creates a new dynamic, and Mastercard's plans for RiskRecon are going to be watched with interest by the rest of the industry. Ratings vendor customers should pay attention to the market activity over the next 12 to 24 months, as your current provider's long-term future may not be as a standalone ratings provider. Market exits and change of focus could impact your current use of these systems. Forrester expects other acquisition activity in 2020, with further consolidation reducing the number of major ratings vendors to three or four by 2025. The industry is developing this way because:

- **CISOs' ability to trust multiple ratings solution vendors is limited.** By nature, security leaders aren't a trusting bunch of professionals. It comes with the territory. Cybersecurity ratings vendors have battled for years to gain acceptance by enough security leaders for the solution category to take off. The largest vendors now have enough customers using cybersecurity ratings that it's unlikely to go away. However, many of the vendors acknowledge the difficulty of gaining CISO trust. One ratings vendor leader remarked, "To gain trust we have had to open up more about how our ratings work and what data we use. Most players in this space now realize that transparency is

FORRESTER®

Forrester Research, Inc., 60 Acorn Park Drive, Cambridge, MA 02140 USA
+1 617-613-6000 | Fax: +1 617-613-5000 | forrester.com

a must-have." Forrester believes this market will see significant consolidation in the next 24 to 36 months as smaller vendors exit into adjacent markets or get acquired by larger market participants. This is also shown in an analysis of client inquiries Forrester conducted in 2019, in which three firms were mentioned in almost all customer-facing conversations.

- **Driving operational improvement will become the major market qualifier for CISOs.** CISOs today have to manually compare ratings data to other data sources they hold. Security leaders don't think this is a good use of their people's time. One US-based security leader told us, "My third-party risk analyst has to manually review a vendor questionnaire and map ratings data to it, which is not a good use of their time." Ratings firms need to make it easier for security leaders to gain insight from the data they hold about organizations. For example, automatic mapping of ratings data to vendor questionnaire submissions helps a firm gain operational insights into where a vendor's statements in a questionnaire (such as "We're always up to date with our patching") don't match externally observable data. Getting better at harnessing this insight and automating it is a key part of most major ratings vendors' roadmaps over the next 12 months.

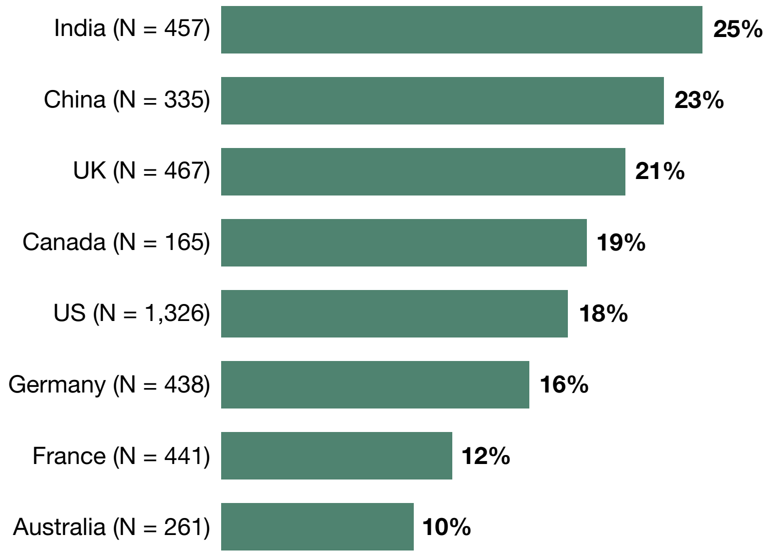
- **Major cybersecurity risk ratings use cases blur with adjacent markets.** The two most common cybersecurity risk rating business uses are third-party risk management and enterprise cyber risk management. As cybersecurity ratings providers integrate into broader business processes, they're seeing vendors in adjacent markets compete with them for business. For example, Recorded Future's Third-Party Risk product and OneTrust's Vendorpedia product offer approaches in third-party risk intelligence not dissimilar to those of existing cybersecurity ratings vendors.[3] Security leaders should also pay attention to Moody's and Team8, which are collaborating to build a cyber risk offering.[4] Expect more of this as smaller vendors in the ratings space pivot to focus on specific use cases and find more success in other market spaces.

- **Some CISOs are driving voluntary internal data sharing with ratings providers.** CISOs who are the most enthusiastic about risk ratings solutions talk about the need for the rating to also take internal security data into account to show effectiveness of internal security controls. The simplicity of the ratings as a board communication tool sparks the desire of CISOs to show how the cybersecurity posture of the firm has changed over time, covering internal and externally observable cyber risk factors. Vendors will examine the potential for doing this subject to the caveats that: 1) they can't compel enterprises or third parties to share this data; 2) it's unlikely to be used in the ratings calculation itself due to the inconsistent nature of what internal data is used across companies; and 3) they will look at data that is consistent across companies (e.g., statements about information security controls and data points used to measure security commonly found in corporate governance sections in Form 10-K filings or the Annual Report on Account).

- **CISOs find cybersecurity ratings valuable, but geographical variations exist.** Security leaders in India, China, the UK, Canada, and the US report finding cybersecurity ratings solutions most valuable in determining security of their supply chain (see Figure 1). Other locations such as Australia, France, and Germany show evidence of lesser penetration of cybersecurity rating solutions, hampered by lack of local language support and skepticism about the value of such solutions. Expect vendors to expand their international language support and relevance to non-English speaking audiences and areas that have not yet had much exposure to these solutions.

FIGURE 1 Security Leaders Who Found Cybersecurity Ratings Valuable For Third-Party Security Management

Percentage of respondents who find security scoring/ratings valuable for managing third-party risk



Base: security decision makers

Source: Forrester Analytics Global Business Technographics® Security Survey, 2019

CISOs Use Ratings Firms To Improve Board-Level Communication

CISOs are reacting to these changes in the market by demanding that firms help them drive simpler board reporting. In addition, security leaders want to move far beyond reviewing ratings data in isolation with manual spreadsheet-driven exercises. CISOs like the simplicity of the rating concept to communicate cyber risk with their boards but need it to be less manually driven. CISOs are reacting to the developing market by:

› **Speaking the language of risk to the board . . .** CISOs have reported that using the cyber rating has proved to be an easy way of communicating the company's cybersecurity posture to senior business leaders. One of the firms interviewed for this research noted, "We gave one of our investors their security rating and the security team within the investor got quite upset initially. They went away and saw that some of the things we had picked up, showed them things they weren't previously aware of." As the concept is simple to understand and clearly shows how performance has improved or gotten worse over time, it has been a mechanism used by some security leaders to break down the technical language associated with security in the boardroom.[5]

› **. . . but being wary of solely using ratings to drive their security programs.** While the rating is valuable for leveling the playing field for board-level discussions about security, it also introduces a moral hazard. Presenting a rating and the security issues that influence it can distract the board of directors so that they focus solely on things that improve the rating. Security leaders must check this tendency: Educate boards that it's a tool to indicate a perspective on the firm's cyber risk, not a latter-day Oracle of Delphi that can predict the future.[6]

› **Driving automation and workflow integration.** Currently, security leaders must do a lot of work to map a cyber rating and its data to their questionnaires. One US-based CISO commented, "I have an analyst that has to look at all of the ratings data and map it to my questionnaire data. That needs to be automated." This manual drudgery is not being tolerated, and ratings vendors are responding to this market need. Expect ratings firms to develop integrations with third-party GRC platforms like MetricStream, RSA Archer, ServiceNow, and other GRC platforms.[7] This will feed data into third-party risk modules and enterprise risk modules directly, mapping questionnaires to data found in GRC platforms.

What It Means

Cyber Ratings Will Become A Vital Boardroom Communication Tool

Cybersecurity ratings are just emerging as tools for talking about cybersecurity risk with the board, having historically been the province of security professionals. Forrester expects cybersecurity ratings to become a de facto standard in the boardroom by 2025. Investors and traditional debt ratings agencies will include cybersecurity as a risk factor for rating the ability to repay company debt (influenced in part by the cybersecurity ratings market). As cybersecurity becomes part of debt financing discussions, directors will expect security leaders to show how their cybersecurity program can help drive down these costs. Security leaders will review cybersecurity ratings during regular board discussions and should expect their cybersecurity program to make ratings improvement part of regular business-as-usual activities.

Supplemental Material

Survey Methodology

The Forrester Analytics Global Business Technographics® Security Survey, 2019, was fielded between April and June of 2019. This online survey included 3,890 respondents in Australia, Canada, China, France, Germany, India, the UK, and the US from companies with two or more employees.

Forrester Analytics' Business Technographics ensures that the final survey population contains only those with significant involvement in the planning, funding, and purchasing of business and technology products and services. Dynata fielded this survey on behalf of Forrester. Survey respondent incentives include points redeemable for gift certificates.

Please note that the brand questions included in this survey should not be used to measure market share. The purpose of Forrester Analytics' Business Technographics brand questions is to show usage of a brand by a specific target audience at one point in time.

Companies Interviewed For This Report

We would like to thank the members of the Forrester Security and Risk Council who attended a roundtable discussion on this topic in September 2019 to discuss cybersecurity risk ratings solutions and offered insights into how they use cyber rating solutions in their security programs.

We would also like to thank the individuals from the following companies who generously gave their time during the research for this report.

BitSight

FICO

Panorays

RiskRecon

SecurityScorecard

Related Research Documents

Cybersecurity Risk Ratings Enhance Third-Party Risk Management

The Forrester New Wave™: Cybersecurity Risk Rating Solutions, Q4 2018

Endnotes

[1] Marmite is a British product based on yeast extract; its marketing campaign is "Love it or Hate it." This is an accurate description of sentiment within the security leadership community for solutions in this space. Source: Arwa Mahdawi, "Marmite: love or hate its PR, you have to admit it's strong stuff," The Guardian, November 30, 2011 (https://www.theguardian.com/commentisfree/2011/nov/30/marmite-love-it-hate-it-pr).

[2] Source: "Mastercard Acquires RiskRecon to Enhance Cybersecurity Capabilities," Mastercard press release, December 23, 2019 (https://newsroom.mastercard.com/press-releases/mastercard-acquires-riskrecon-to-enhance-cybersecurity-capabilities/).

[3] Source: "Security Intelligence for Third-Party Risk," Recorded Future (https://www.recordedfuture.com/solutions/third-party-risk/).

Source: "Vendor & Third-Party Risk," OneTrust (https://www.onetrust.com/solutions/vendor-third-party-risk/).

[4] Source: Tova Cohen and Ari Rabinovitch, "Moody's, Israel's Team8 to create cyber risk standard for businesses," Reuters, June 27, 2019 (https://uk.reuters.com/article/us-cyber-moody-s-team8/moodys-israels-team8-to-create-cyber-risk-standard-for-businesses-idUKKCN1TS09N).

[5] See the Forrester report "How To Talk To Your Board About Cybersecurity."

[6] The Oracle of Delphi in Pythia, Greece was a mythical high priestess who was said to be able to foretell the future by direct discussion with the Greek God Apollo. Source: Gabriel H. Jones, "Pythia," Ancient History Encyclopedia, August 30, 2013 (https://www.ancient.eu/Pythia/).

[7] RSA is due to be divested from Dell and sold to a private equity firm: Symphony Technology. Source: Ron Miller, "Dell sells RSA to consortium led by Symphony Technology Group for over $2B," TechCrunch, February 19, 2020 (https://techcrunch.com/2020/02/18/dell-sells-rsa-to-consortium-led-by-symphony-technology-group-for-over-2b/).

FORRESTER®

forrester.com

We work with business and technology leaders to drive customer-obsessed vision, strategy, and execution that accelerate growth.

PRODUCTS AND SERVICES

- Research and tools
- Analyst engagement
- Data and analytics
- Peer collaboration
- Consulting
- Events
- Certification programs

Forrester's research and insights are tailored to your role and critical business initiatives.

ROLES WE SERVE

Marketing & Strategy Professionals

CMO

B2B Marketing

B2C Marketing

Customer Experience

Customer Insights

eBusiness & Channel Strategy

Technology Management Professionals

CIO

Application Development & Delivery

Enterprise Architecture

Infrastructure & Operations

› Security & Risk

Sourcing & Vendor Management

Technology Industry Professionals

Analyst Relations

CLIENT SUPPORT

For information on hard-copy or electronic reprints, please contact Client Support at +1 866-367-7378, +1 617-613-5730, or clientsupport@forrester.com. We offer quantity discounts and special pricing for academic and nonprofit institutions.