Response from SecurityScorecard

Comment on
RIN 3235-AN08 ("Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies")

I. Introduction

SecurityScorecard, the global leader in cybersecurity ratings, welcomes the opportunity to comment on the Securities and Exchange Commission's (SEC) proposed rule on cybersecurity risk management for investment advisers, registered investment companies, and business development companies.[1] The SEC's work in this area is critical as cybersecurity risks to businesses grow and executives, shareholders and customers seek greater clarity about appropriate approaches to cybersecurity risk management.

In this submission, we review why third-party security ratings and assessments are a cost-effective, comprehensive, and standardized way for organizations to assess and manage their cybersecurity risks. We also recommend that the SEC:

- Require that advisers' and funds' cybersecurity policies and procedures include third-party risk assessments (responding to Question 3);
- Recognize that third-party assessments that produce security ratings are a cost-effective, comprehensive, and standardized way for organizations to assess and manage their cybersecurity risks, given half of all data breaches occur through third-party connections (responding to Question 9);
- Require that organizations conduct assessments of their information systems on a continuous basis (responding to Question 11);

[1] RIN 3235-AN08. Cybersecurity Risk Management for Investment Advisers, Registered Investment Companies, and Business Development Companies.

- Require advisers and funds to assess the compliance of all service providers as listed, by leveraging cybersecurity risk assessments and security ratings (responding to Question 14);

- Require advisers' and funds' cybersecurity policies and procedures to include oversight of certain providers—including pursuant to written contracts (responding to Question 17);

- Recognize that advisers and funds can obtain information from or about their service providers' cybersecurity practices through cybersecurity assessments and security ratings in a cost-effective manner (responding to Question 19);

- Recognize that continuous monitoring is a best practice for managing cybersecurity risk, and that security ratings are a cost-effective contributor to continuous monitoring (responding to Questions 20-25); and

- Recognize that security ratings are a free, cost-effective source of data for boards on a fund's cybersecurity risk management posture (responding to Questions 26-32).

II. Security Ratings and Continuous Monitoring for Cyber Threats

In its proposed rule, the SEC seeks to require covered advisers and funds to implement cybersecurity policies and procedures to reduce risk.[2] The SEC's proposed rule focuses, in part, on requiring registered investment advisers and investment companies to "adopt and implement written cybersecurity policies and procedures reasonably designed to address cybersecurity risks."[3] Before companies can address cybersecurity risks, however, they must first understand what the risks are. Security ratings provide that awareness. That is why SecurityScorecard believes that security ratings are a necessary component for every cybersecurity policy and should be a required element of this rule.

As Cybersecurity and Infrastructure Security Agency (CISA) Director Jen Easterly testified to Congress in 2021, "I think it's hard to say you've reduced risk unless you know how to measure it." SecurityScorecard wholeheartedly agrees. You can't manage what you can't measure, and you can't defend what you can't see. The cyber threat environment is constantly evolving, organizations' IT environments are constantly evolving as well, and many organizations are nearly blind to their third-party risk even though over half of all cyber incidents occur through third-party digital connections.[4] To manage all this cybersecurity risk, organizations cannot use a playbook that relies on static analyses and entirely qualitative objectives. Instead, they must continuously assess cybersecurity risk across their entire supply chain and vendor ecosystem and produce quantitative metrics to measure that dynamic risk in a standardized, actionable way. This is what security ratings deliver.

Third-party assessments provide unique, valuable insights and metrics on an organization's cybersecurity posture and the credibility of its claims about that posture. When conducted independently, assessments validate for the public, third-party organizations, and regulators that an organization is employing adequate cybersecurity measures. Especially when organizations are sourcing network and internet infrastructure components from a diverse and distributed global supply chain, third-party assessments can help an organization understand how these components affect its exposure to cybersecurity risks—to identify, analyze, and then mitigate those risks. As part of this process, security

[2] Ibid., 1.
[3] RIN 3235-AN08. 1.
[4]

ratings provide organizations with quantifiable cybersecurity metrics that can be easily communicated and compared against other similar metrics.

For example, among the ten risk group factors analyzed and scored in our ratings is a patching cadence module, which analyzes how quickly an organization installs security updates to measure vulnerability risk mitigation practice efficacy. Patching is a critical component of preventative maintenance for computing technologies, and a way to increase resilience and secure information systems. In Fig. 1 (Patching Cadence Scorecard - Medium Severity), we show an example of how our platform quantifies risk related to patching cadence; sorts risks by CVSS severity; and provides clear metrics for IT, C-suite, and Board of Director leadership to track patching cadence across the enterprise system.

SecurityScorecard's A-F security ratings platform offers rigorous, free cybersecurity self-assessments to customers, and cost-effective assessments for their third-party vendors and suppliers. We conduct daily scans of the entire internet to map cybersecurity risk exposure and bring transparency to an

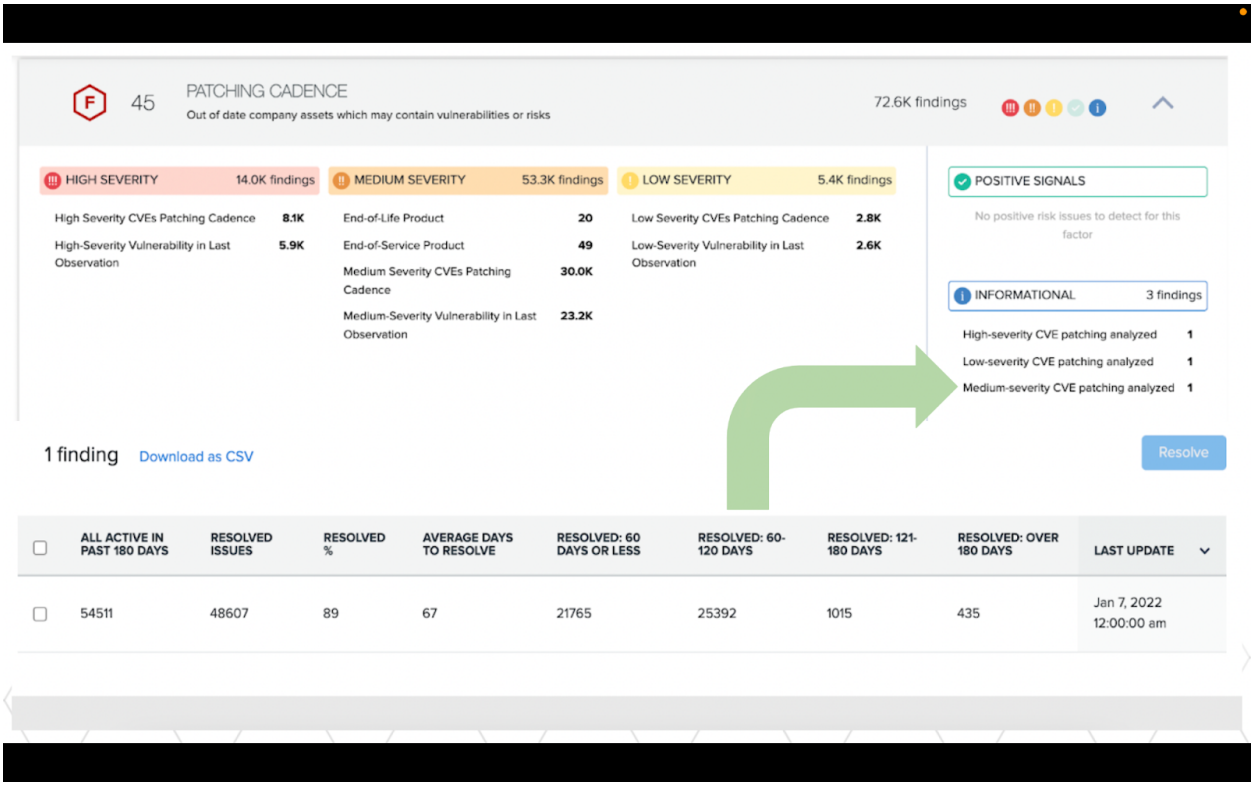

Figure 1

organization's cyber hygiene. We do this without going behind any firewalls, only collecting public-facing data. We offer an "outside-in" perspective on an organization's security posture: we give organizations the ability to see what a hacker would see and are thus able to generate insights about the vulnerabilities, active exploits, and advanced cyber threats that a specific organization faces. Our customers use our platform not only to identify weaknesses in their own enterprise cyber hygiene, but to support their vendor risk management and supply chain security initiatives as well.

We generate our ratings (i.e., scores) by drawing on publicly available information, weighted and combined with historical data, to produce an objective security score. Importantly, this score, and the analytics behind it, change dynamically in response to changes in an organization's exposure to risks: if an organization's cyber hygiene starts to deteriorate, its score will suffer. While a high score does not translate to immunity from cyber risk, poor scores are strongly correlated with increased likelihood of breach. This is unsurprising, as a poor score reflects that an organization has not sufficiently hardened its infrastructure against malicious actors. [See Fig. 2]

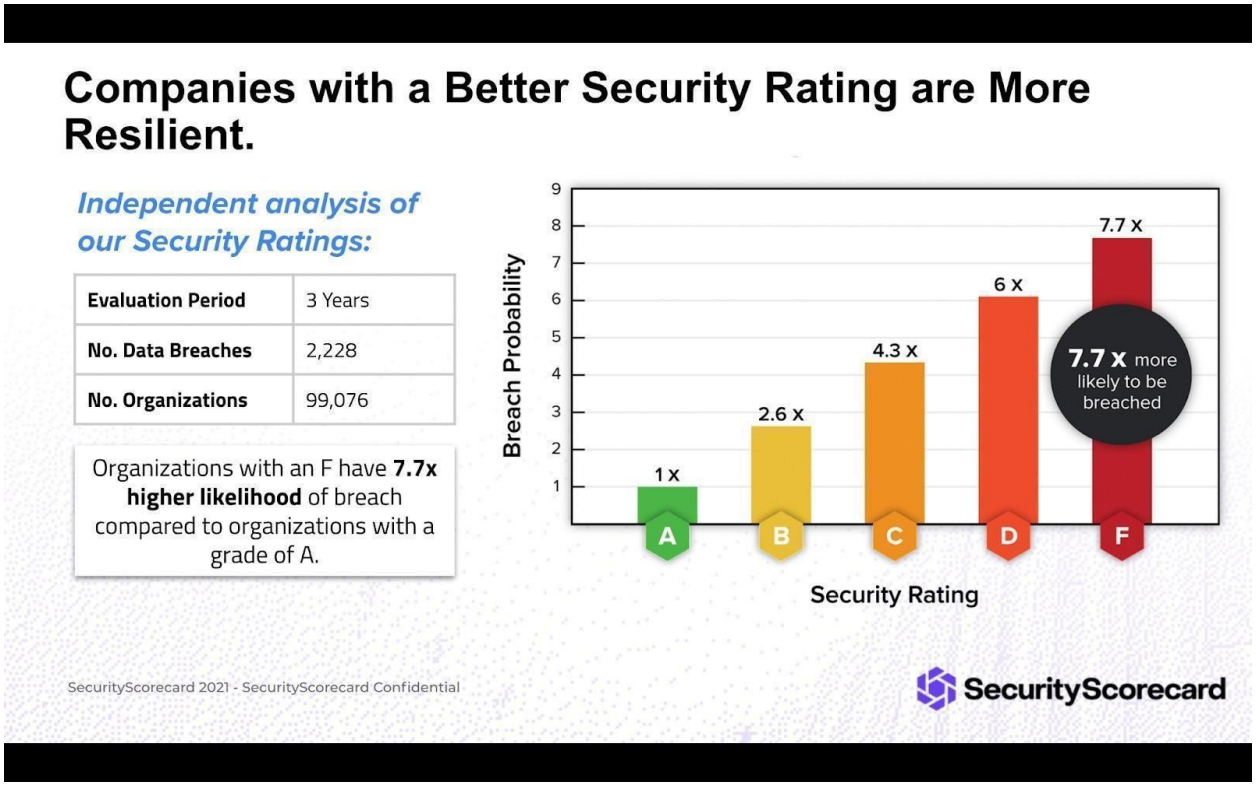

Figure 2

We offer a comprehensive picture of their risk landscape alongside standardized, actionable security metrics. This kind of solution empowers organizations to accomplish many tasks:

- Continuously monitor their entire cyber risk exposure, including third-party vendors and suppliers;
- Choose the right Key Performance Indicators (KPIs) to prioritize and address cyber risk;
- Evaluate the effectiveness of existing internal security controls, tools, and processes;
- Identify potential gaps in security;
- Track remediation and mitigation efforts in real-over time;
- View cybersecurity progress improvements over time;
- Monitor and compare performance with industry competitors;
- Oversee third-party vendor cybersecurity; and
- Improve communication with vendors, regulators, and the board.

Security ratings are also cost-effective. Any organization can access their own security rating for free and scale their vendor risk management program to meet their needs. This is especially valuable for small- and medium-size businesses as well as local governments, who may not have the resources to employ a dedicated IT team or to contract IT services to defend their networks from cyber- and vendor-related risks. We can also help organizations to tailor their continuous monitoring and security metrics to their specific business needs. Security ratings are additionally cost-effective because they help build long-term capacity to manage cyber risk. As cyber threats evolve and as the IT environment changes, organizations can easily update security metrics in response—because they already have a risk assessment and security metrics framework in place.

For these reasons, security ratings are rapidly emerging as an essential element of cybersecurity risk management. According to CISA's then-Assistant Director for the National Risk Management Center:

> "The emergence of security ratings has driven cyber risk quantification as a way to calculate and measure cyber risk exposure. These security ratings provide a starting point for companies'

> cybersecurity capabilities and help elevate cyber risk to board decision making. Entities can also use security ratings alongside strategic risk metrics to align cyber scenarios with material business exposure; rollup cyber risks with financial exposure to inform risk management decisions; and measure improvement of cyber risk reduction over time. This kind of work needs to happen in the boardroom and also amongst national security leaders."

III. Recommendations

Independent assessments and security ratings should be an essential element of any organization's comprehensive strategy for managing cyber risks. Interconnected technology infrastructure sourced from a distributed, global, and diverse supply chain brings many possible risks. Organizations may not trust the risk assurances given by a particular provider, and organizations in general may lack a comprehensive understanding of where a technology came from and its embedded risks. Third-party assessments with security ratings also enable organizations to understand their own risk posture—screening an entire organization's digital and contractor supply chain to identify risks and quantitatively measure them.

Importantly, these measurements are cost-effective: technologies to perform them are widely available, and once organizations conduct one such assessment, subsequent assessments can build on those ratings to continually update cybersecurity risk assessments.

Third-party assessments, such as the security ratings offered by SecurityScorecard, can help advisers and funds protect themselves and their customers against cybersecurity risks. Getting a more comprehensive, quantitative picture of an organization's digital supply chain empowers that organization to identify and target cybersecurity risks. Security ratings can also ensure that organizations better understand their network technologies while they procure them, before they deploy them, and as they maintain them. Further, security ratings provide a measurable, standardized, and cost-effective way of assessing an organization's cybersecurity, including vis-à-vis their contractor and digital supply chains.

"Question 3: Are the proposed elements of the cybersecurity policies and procedures appropriate? Should we modify or delete any of the proposed elements? Why or why not? …"

Accordingly, we recommend, in response to Question 3, that third-party risk assessments be a required element of advisers' and funds' cybersecurity policies and procedures. Security ratings are a cost-effective risk assessment tool that furnishes organizations with quantitative insights about their cybersecurity risk posture. The SEC could even consider requiring companies to maintain a minimum rating that corresponds to statistical performance benchmarks. For example, SecurityScorecard finds that organizations with a "B" rating are 50% less likely to be breached than those with an "F" rating.

"Question 9: What are best practices that commenters have developed or are aware of with respect to the types of measures that must be implemented as part of the proposed cybersecurity risk management rules…?"

In response to Question 9, the SEC should recognize that third-party assessments that produce security ratings are a cost-effective, comprehensive, and standardized way for organizations to assess and manage their cybersecurity risks, given half of all data breaches occur through third-party connections.[5] On that basis alone, requiring organizations to assess the cybersecurity risk posed by vendors, contractors, and other third-party relationships would greatly enhance their cybersecurity posture. Conversely, when organizations like advisers and funds do not employ vendor risk management processes, they overlook half of their risk exposure. Assessing individual vendor relationships at the product and/or service level, defining

[5] "51% of organizations have experienced a data breach caused by a third-party," *Security Magazine*, May 7, 2021, https://www.securitymagazine.com/articles/95143-of-organizations-have-experienced-a-data-breach-caused-by-a-third-party.

vendor performance metrics, creating robust vendor contracts, and establishing clear lines of communication between vendors and the organization's board, among others, can all help bolster this vendor risk management.

"Question 11: ...Should the proposed rules specify a minimum assessment frequency, and if so, what should that frequency be?"

In response to Question 11, we recommend that organizations should be required to conduct assessments of their information systems on a continuous basis. As we have emphasized throughout this submission, continuous monitoring tools are cost-effective and produce easily understandable security ratings that decision-makers can use in real-time. Further, the threat landscape is not static—and organizations face new risks as cyber threat actors evolve their tactics and as organizations' technology environments change. The cost-effectiveness and availability of security assessment technology means organizations should be continuously monitoring their own cyber hygiene.

"Question 14: Should we require advisers and funds to assess the compliance of [relevant service providers]…with these proposed cybersecurity risk management rules?"

In response to Question 14, we recommend that the SEC require advisers and funds to assess the cybersecurity risk posture of all service providers as listed—those "that receive, maintain, or process adviser or fund information, or are otherwise permitted to access adviser or fund information systems and any adviser or fund information residing therein." Organizations increasingly source technology and services from a global, distributed, complex, and entangled digital supply chain which can bring with it all matters of risks. Security ratings are a cost-effective way for any organization to assess and monitor cybersecurity risk, including risk associated with service providers—empowering the organization to select the best third-party service providers for their cybersecurity posture.

"Question 17: Should we require advisers' and funds' cybersecurity policies and procedures to require oversight of certain service providers, including that such service providers implement and maintain appropriate measures designed to protect a fund's or an adviser's information and information systems pursuant to written contract? …"

In response to Question 17, we recommend that the SEC should require advisers' and funds' cybersecurity policies and procedures to require oversight of certain providers—including pursuant to written contract. Policies to require oversight of service providers is critical in a world in which more than half of cyber incidents occur through third-party connections. Security ratings provide a cost-effective continuous monitoring capability.

"Question 19: Are advisers and funds currently able to obtain information from or about their service providers' cybersecurity practices (e.g., policies, procedures, and controls) to effectively assess them?"

We comment, in response to Question 19, that advisers and funds can obtain information from or about their service providers' cybersecurity practices through cybersecurity assessments and security ratings. Technological advancements have increasingly made these security ratings quicker and more cost-effective to produce—as well as more comprehensive. Organizations can leverage these technologies to produce quantifiable metrics on their service providers' cybersecurity practices, which in turn can be used to make purchasing, contracting, and other business- and cybersecurity-related decisions.

Questions 20-25: Annual Review and Required Written Reports

In Questions 20-25, the Commission requests feedback on how often advisers and funds should review their cybersecurity policies and procedures to ensure that they reflect changes in cybersecurity risk—and how significant a burden an annual or other review would impose on advisers or funds. We acknowledge that full-blown examinations, audits, and executive attestations may be costly for many advisers and funds. That said, as we have emphasized throughout this submission, continuous monitoring is a best practice for managing cybersecurity risk, and security ratings are a cost-effective contributor to continuous monitoring.

Questions 26-32: Fund Board Oversight

Security ratings are a rich source of data for boards on a fund's cybersecurity risk management posture. Security ratings clearly articulate an organization's risk posture—including the risk posture of related third parties—in an easily understandable fashion. They also enable individuals, like those sitting on a board, to compare an organization's cybersecurity posture and risk management program with that of other organizations.

Respectfully submitted,
SIGNED