Response from SecurityScorecard

Notice, Request for Information on
Evaluating and Improving NIST Cybersecurity Resources: The Cybersecurity Framework and Cybersecurity Supply Chain Risk Management

I. Introduction

SecurityScorecard, the global leader in cybersecurity ratings, welcomes the opportunity to respond to the National Institute of Standards and Technology (NIST)'s notice and request for information (RFI) on evaluating and improving NIST cybersecurity resources,[1] including supply chain risk management. NIST's work on supply chain risk management is critical as increasingly complex, entangled, and globally distributed supply chains expose organizations to a myriad of cybersecurity risks. As the RFI highlights, adapting cybersecurity frameworks and best-practices to the changing technology landscape is vital for risk management. In this submission, we offer specific feedback on how security ratings, a widely available and cost-effective tool, can reduce cybersecurity risk and improve management of that risk.

Third-party security ratings and assessments are a cost-effective, comprehensive, and standardized way for organizations to assess and manage their cybersecurity risks, including risks originating in their supply chains. NIST has already recognized the positive impact security ratings can have on supply

[1] Evaluating and Improving NIST Cybersecurity Resources: The Cybersecurity Framework and Cybersecurity Supply Chain Risk Management. 220210-0045. *Federal Register*, Vol. 87, No. 35, February 22, 2022, 9579.

chain security in its draft SP 800-161 Rev 1 document published on October 18, 202, categorizing it as a "foundational capability"for enhanced vendor risk assessments. We urge NIST to continue recognizing the importance and utility of security ratings as a foundational capability not only to reduce supply chain risk, but as a core tool to inform and prioritize decisions regarding cybersecurity. We offer the following recommendations:

- In response to Question 3, we emphasize the cost-effectiveness of security ratings;
- In response to Question 11, we recommend that additional NIST resources explicitly incorporate the importance of continuous monitoring and cybersecurity metrics into NIST documentation; and
- In response to Question 12, we recommend that NIST resources emphasize the availability and cost-effectiveness of continuous monitoring and independent, third-party cybersecurity risk assessments, noting recent technological developments, like security ratings, have lowered the cost and increased the value-add of producing such metrics.

II. Security Ratings and Continuous Monitoring for Cyber Threats

In the request for information, NIST asks for input on ways to improve the agency's cybersecurity resources and its work on supply chain risk management. This includes evaluations of the NIST Cybersecurity Framework, possible updates to the Framework to account for new cybersecurity risks and technologies, and focus areas for the newly announced National Initiative for Improving Cybersecurity in Supply Chains (NIICS) to address cybersecurity risks in supply chains. Specifically, it asks whether NIST should update the Cybersecurity Framework and other NIST cybersecurity resources to account for new technological changes, new cybersecurity risks and resources, and issues of supply chain risk management in general.

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.[2] 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 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.

---

[2] "51% of organizations have experienced a data breach caused by a third-party," *Security Magazine*, May 7, 2021.

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 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.

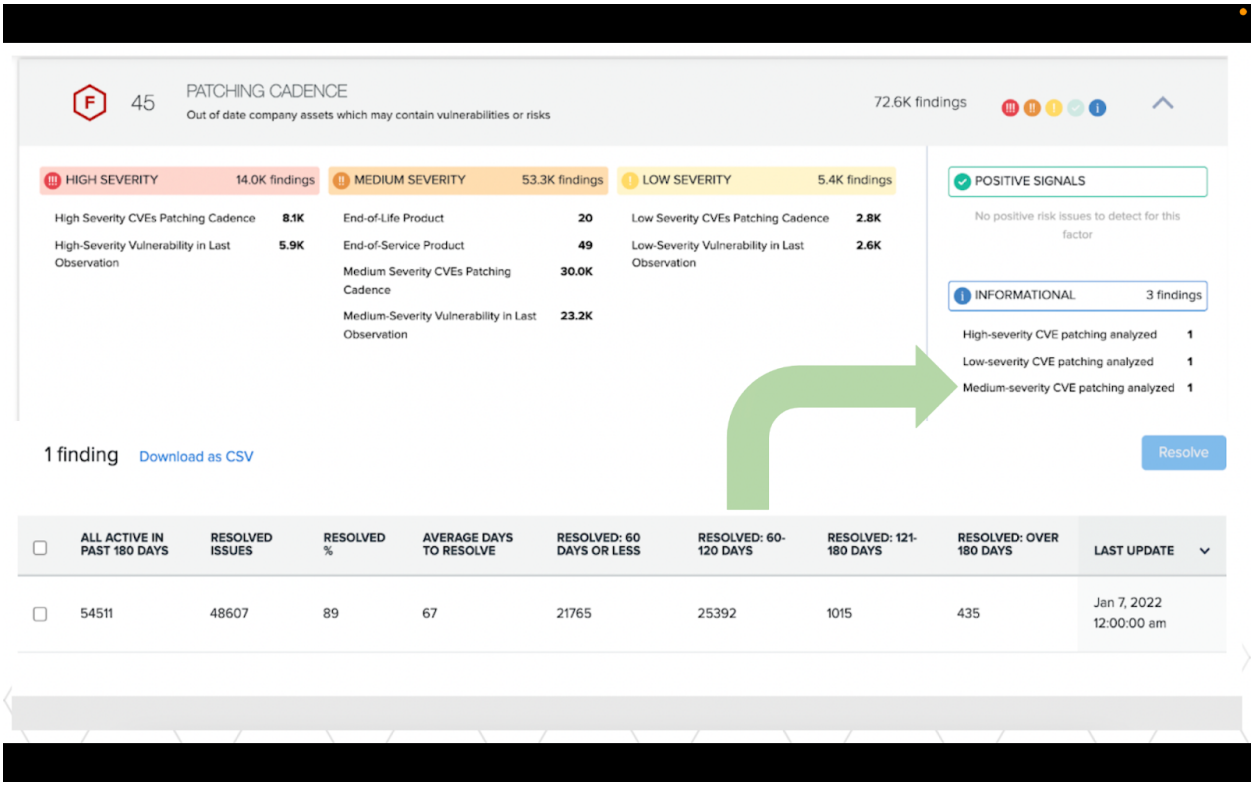

Figure 1: Patching Cadence Scorecard - Medium Severity

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, as the data in Fig. 2 reveals.

Figure 2

We offer a comprehensive picture of an organization's 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

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. Static, point-in-time assessments of cybersecurity provided

by a supplier are inadequate in a constantly evolving threat environment, and organizations in general may lack a comprehensive understanding of where a technology came from and its embedded risks. 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.

3. Challenges that may prevent organizations from using the NIST Cybersecurity Framework or using it more easily or extensively (e.g., resource considerations, information sharing restrictions, organizational factors, workforce gaps, or complexity).

Resource constraints–and knowing how much investment in risk mitigation is enough–are perennial challenges for all organizations, regardless of size. Importantly, many security ratings companies provide their ratings to organizations for free;[3] 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 organizations 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.

11. National Initiative for Improving Cybersecurity in Supply Chains (NIICS). What are the greatest challenges related to the cybersecurity aspects of supply chain risk management that the NIICS could address? How can NIST build on its current work on supply chain security, including software security work stemming from E.O. 14028, to increase trust and assurance in technology products, devices, and services?

Accordingly, we recommend, in response to Question 11 about building on

[3] "Cyber Security Ratings," Free Cybersecurity Services and Tools, the Cybersecurity and Infrastructure Security Agency, accessed online Apr. 20, 2022, https://www.cisa.gov/free-cybersecurity-services-and-tools.

E.O. 14028 and other current work, that NIST explicitly incorporate the importance of continuous monitoring, security ratings, and cybersecurity metrics into more of its documentation. Continuous monitoring empowers organizations to adapt to evolving technological environments, a changing threat landscape, and even new business and regulatory demands. Critically, it also gives an organization visibility into its vendor risk. Over 50 percent of cyber incidents occur through third party connections, yet companies still rely on occasional, static, point-in-time assessments of their vendors. As a result, companies have much less than full visibility of their attack surface.

Metrics are also a cost-effective way for organizations to quantify cybersecurity risk, better communicate that risk to stakeholders (from company attorneys to board members), and compare their risk posture against their history and that of their vendors. They are essential components of building out comprehensive supply chain risk management programs.

12. Approaches, tools, standards, guidelines, or other resources necessary for managing cybersecurity-related risks in supply chains. NIST welcomes input on such resources in narrowly defined areas (e.g. pieces of hardware or software assurance or assured services, or specific to only one or two sectors) that may be useful to utilize more broadly; potential low risk, high reward resources that could be facilitated across diverse disciplines, sectors, or stakeholders; as well as large-scale and extremely difficult areas.

We also recommend, in response to Question 12 about new resources to manage supply chain risk, that NIST give a more central role in its frameworks to continuous monitoring and independent, third-party cybersecurity audits. These audits allow organizations to better assess their own supply chain, from third-party software applications to vendor touchpoints, and they can also help organizations to better risk-assess specific technologies that come from a complex, global supply chain. Moreover, continuous, independent security audits can support other parts of the NIST Cybersecurity Framework.

Generating standardized cybersecurity metrics enables organizations to better

quantify their risk posture and to contextualize their supply chain vulnerabilities within their broader cybersecurity risk management policies and processes. Recent technological developments have lowered the cost and increased the value-add of producing such metrics.

Respectfully submitted,
SIGNED