Security Ratings: A Tool as Part of a Risk Management Program

American Bankers Association®

Security Ratings: A Tool as Part of a Risk Management Program

As the world becomes more connected and the threat in cyber space continues to grow, financial institutions (FIs) have worked to more efficiently and effectively understand their own risk, as well as those of third parties or other supply chain players.

A number of providers now offer security ratings, also referred to as risk scores or risk ratings, as a way to measure an organization's cybersecurity hygiene. They aim to provide a method for comparing two or more organizations on their cybersecurity implementation by using the same standards and controls. For businesses that are looking to evaluate their own security posture, or the risk exposure created by third parties, the existence of a single metric embodying the effectiveness of a cybersecurity program is a welcome development. The promise of a single score or rating, a financial institution can use to make an "apples to apples" comparison and objectively determine which third party potentially poses more risk of harm is enticing. **Unfortunately, due to the inherent limitations, a security rating cannot provide a full picture of an organization's cybersecurity program.** However, they can provide valuable insight as part of a risk management program.

Security rating providers use a combination of data points collected or purchased from public and private sources and proprietary algorithms to articulate an organization's security effectiveness into a quantifiable measure or score. As these ratings rely in part on the quality and breadth of the data they use, the variety of sources they consult and the dynamic nature of the environment they operate in, these ratings can potentially be inaccurate, irrelevant or incomplete. The goal of this paper is to help financial institutions understand what security ratings are, how they can be used as part of a risk management program, and identify other tools that can supplement security ratings.

How do Security Ratings Work?

Each security rating provider has its own proprietary methodologies and algorithms that support their product, but they share many commonalities in terms of process and data sources.

1. Evaluate public internet-facing assets of an organization.

Pros:

- Because this is a non-cooperative process, the providers can produce ratings on any organization that connects to the internet.
- This data can be purchased with in-house capabilities and can be refreshed on a regular basis (as frequently as daily or weekly) ensuring the timeliness of the data and ratings.

- Firms can have access to security data on organizations in the absence of having a direct contractual relationship (e.g., supply chain providers).

Cons:

- The entire basis of an organization's rating depends on the ability of the rating provider to accurately attribute the scanned Internet Protocol (IP) addresses to an individual organization.
    - Due to the scale of these scans, they are automated processes. While there are multiple ways to gather this information and assign an IP to an organization, it is nearly impossible to do this with a 100% accuracy. Thus, some IPs assigned to an organization, and included in the rating, may not belong to that organization while others that belong to an organization may not be included.
    - Some organizations have incredibly complex network topologies due to the nature or size of their business. This may include segmented networks that operate at different security levels. These scans have no way to differentiate between a network connected directly to critical networks versus those that are being held for future use and are not used or connected to critical information. As all IPs are treated equally in the ratings, this can result in unused IPs decreasing the rating of an organization, which may have implemented internal controls (e.g., disconnecting from critical networks) to account for this risk in the absence of costly controls.
    - Recognizing the criticality of getting the IP assignation process correct some providers claim to validate the information -- but without a cooperative process in place with the evaluated organization -- it is virtually impossible to ensure 100% accuracy.
- The public internet-facing methodology does not account for the internal security protocols in place.
    - Good cybersecurity relies on a layered approach and any activities that occur "inside the fence line" are not accounted for as part of these ratings, such as network segmentation, employee training, and approaches to authentication.
    - For financial institutions that are required[1] to implement an information security program based on risk to protect sensitive information, this includes implementing layered controls. These programs and

[1] As mandated by Section 501 of the Gramm–Leach–Bliley Act of 1999 and the implementing "Guidelines Establishing Standards for Safeguarding Customer Information" released by Federal banking regulators and the "Safeguards Rule" released by the Federal Trade Commission.

underlying controls are evaluated through routine examinations by Federal regulators. External-facing methodologies are not able to accurately measure an institution's cybersecurity capabilities and culture without an understanding of the full program.

2. Analyze configuration of services, protocols and patching level and cadence of IP address space assigned to an organization.

Pros:

- Good "cyber hygiene" is an essential part of a layered approach to cybersecurity. A public-facing scan can identify if an organization is employing best practices and reducing vulnerabilities through proper network configuration, patch management, and maintenance of website certificates.
- It is possible to argue that a significant number of unpatched systems or a large number of expired certificates, while potentially not a critical failure, could point to a lax culture of cybersecurity that could be reflected in the internal procedures and protocols and there is an increased likelihood of a critical vulnerability being available or left open.

Cons:

- Assuming the providers have identified correct IPs for an organization, not all networks, especially for more complex or large organizations, are created equal or receive an equal level of maintenance. Therefore, it is quite possible that an organization may have prioritized its maintenance strategies to focus on critical systems—and not on unused or non-critical systems—creating a misleading view of how well an organization maintains its systems when they are scanned.

3. Analyze end-point behaviors to determine if any of the assigned IPs are infected or hosting botnets or malware servers.

Pros:

- While this type of activity can be hard to detect, and again assuming the scans have properly attributed the correct IPs, hosting this type of activity on a network is clearly an area for serious concern and is unambiguously bad.
- Many scoring providers will provide the numbers and levels of infection, which can identify if this activity is an anomaly or endemic and of significant concern.

Cons:

- This type of activity can be challenging to identify and detect. Some organizations have in-house capabilities to track malware-based network traffic and others purchase it from vendors, but it's possible that this type of activity could be missed on a public-facing scan.
- An analysis of IP traffic may misattribute the risk in shared hosting environments. IP traffic in an environment that hosts multiple organizations may not show the victim of malware that affects a subset of those in the shared environment.

4. Assess whether any current proprietary information, usernames or passwords are available on nefarious websites or the dark web based on reported or historical incidents.

Pros:

- Overall risk is based on inherent risk and the supplemental controls that reduce an organization's overall risk. Use of reported incidents and the identification of breached data provides an awareness of inherent risk to an individual organization.
- The independent service continually monitors any organization a company may be interested in that tracks whether that organization has announced an incident or an incident has been reported. These daily or weekly scans will provide relatively quick notice of a change in status that may or may not be provided by the organization themselves.

Cons:

- Certain business types have a more prevalent number of reported breaches, due to regulatory requirements which differ based on firm type and geographic regions. As such, risk ratings that are based on publicly-disclosed incidents will show a greater risk for organizations, such as financial institutions, that have stronger regulatory reporting requirements.
- It is valuable to know if an organization's proprietary data is for sale on the dark web, but depending on the timing of the discovery of this information, it may be more of a forensic tool than a proactive defensive capability.
- Additionally, some security rating providers are attempting to correlate historical breach and metric data with algorithms that try to develop the risk of future breaches occurring based on current measurements and an organization's demographic information. This type of breach precognition is still in its early stages and is constrained by issues like misattribution of IP space, lack of

information on layered defensive measures employed internally, and the regulatory regime and exam structure financial institutions operate under.

How Should Security Ratings Be Employed?

As with all risk management techniques, there is no "silver bullet" for analyzing cybersecurity risk. An overreliance on ratings, can result in an institution making a misinformed decision, since the ratings can only show a perspective on the externally-facing controls with no inclusion of internally layered controls that protect an organization. Instead, security ratings are most useful as part of a broader risk management program. This may include building them into existing programs, such as, third party or vendor management, supply chain risk management, or the institution's own cyber risk management program.

Specifically, firms may use these ratings to:

- Understand potential risk with future partners
- Trigger in-person assessments of a third party on a more frequent basis
- Evaluate the risk of the vendors to third parties
- Identify the firm's weaknesses from an outsider, or attacker's, perspective

The challenges with overreliance on a security rating are outlined in the section "How Do Security Ratings Work?"

Building the ratings into a broader program allows the firm to make decisions accounting for the layered approach to an organization's security program. Security ratings are best used as an important first step with vendors, service providers and partners to evaluate the status of their cybersecurity programs. Security ratings should never be used as a sole data point and should be evaluated in conjunction with other data points. They can help with the initial vetting of potential partners, but given their potential for error, they should not be used as a determining factor on whether to engage in a relationship or not. Additionally, the continual nature of the scanning that informs these scores makes them useful as a tool in an ongoing third party risk management program. A significant negative change in an existing vendor's score can be used as a trigger to investigate the vendor and determine what may have caused the change. This type of capability can be especially useful if an organization is large and engages hundreds or even thousands of vendors.

In addition, the ratings should not be used as the sole factor for determining cyber insurance policies or investor ratings. Ratings may be helpful to build into the analysis but are only valuable when paired alongside a more holistic evaluation of a firm's cybersecurity risk management program.

These ratings can also be part of an ongoing third party risk management program. The continuous nature of the scanning that informs these scores makes them useful as a tool to detect changes in a third parties' external-facing assets. A significant negative change in an existing vendor's score can be used as a trigger to investigate a vendor and determine what may have caused the change. This type of capability can be especially useful if an organization is large and engages hundreds or even

thousands of vendors. If a firm chooses to integrate security ratings into a third party risk management program, they should ensure that providers adhere to the following principles[2]:

- **Transparency:** Rating companies shall provide sufficient transparency into the methodologies and types of data used to determine their ratings, including information on data origination as requested and when feasible, for customers and rated organizations to understand how ratings are derived. Any rated organization shall be allowed access to their individual rating and the data that impacts a change in their rating.
- **Dispute, Correction and Appeal:** Rated organizations shall have the right to challenge their rating and provide corrected or clarifying data. Rating companies should have an appeal and dispute resolution process. Disputed ratings should be notated as such until resolved.
- **Accuracy and Validation:** Ratings should be empirical, data-driven, or notated as expert opinion. Rating providers should provide validation of their rating methodologies and historical performance of their models. Ratings shall promptly reflect the inclusion of corrected information upon validation.
- **Model Governance:** Prior to making changes to their methodologies and/or data sets, rating providers shall provide reasonable notice to their customers and clearly communicate how announced changes may impact existing ratings.
- **Independence:** Commercial agreements, or lack thereof, with rating companies shall not have direct impact on an organization's rating; any rated organization will be able to see and challenge their rating irrespective of whether they are a customer of the rating provider.
- **Confidentiality:** Information disclosed by a rated organization during the course of a challenged rating or dispute shall be appropriately protected. Rating providers should not publicize an individual organization's rating. Rating providers shall not provide third parties with sensitive, non-public information on rated organizations that could lead directly to system compromise.

Additional Tools to Assess Cyber Risk Management

Since security ratings can only evaluate the external-facing assets of a firm and have no insight into a firm's internal controls or any layered approach to cybersecurity that may have been implemented, additional assessments are needed to properly evaluate cyber risk. These assessments could be conducted through an in-depth evaluation of a firm or through common questionnaires or outsourcing.

For firms that have a large number of vendors and third party providers, security ratings could be used to triage their more in-depth analyses. A second part of the triage process should include a

[2] Chamber of Commerce "Principles for Fair and Accurate Security Ratings"

careful examination of the types of data that are shared with each provider and the level of access the provider has to critical systems. For those providers that have access to a firm's critical information or systems, it is essential that a firm fully understand the cybersecurity program in place. It is also critical that their evaluation includes a review of the provider's external and internal controls so that a true evaluation of cyber risk can be accomplished. Using an outside party to gather and validate information enables financial institutions to make more informed decisions about third parties based on an analysis of the layered controls that may be in place within the institution.

Recognizing the challenges and costs of performing due diligence on third parties, some financial institutions have invested in products to help reduce this burden. There are a number of solutions available for banks and two platforms started by financial institutions are KY3P and TruSight. These programs provide an internal review of third parties in an efficient manner by standardizing their reviews of internal account controls and layered risk management approaches. Financial institutions should look closely at increasing scrutiny for their more critical providers, such as those who access critical data or systems. These types of standardized programs reduce duplication of assessments and overhead costs for institutions by allowing for more thorough and frequent assessments.

Conclusion

Security rating providers promise to deliver vetted, validated, updated, and consistent ratings of potential third parties at a low price and with the push of a button. Unfortunately, the reality is a lot more complicated. These ratings do not provide a panacea, and, in fact, may give a false sense of security -- or concern -- about a vendor. As such, the ratings should be used with caution and only as a starting point when evaluating cybersecurity programs. The ratings provider's inability to access internal infrastructure and evaluate internal controls along with the errors inherent in assigning IP space to an individual organization can only provide a superficial view of the cybersecurity program in place. To develop a truly useful assessment of an organization's cybersecurity risk management program requires more detailed information, including an analysis of the internal controls and environment across the entire infrastructure, not just the public-facing assets.