Brown University, Executive Master in Cybersecurity

Critical Challenge Project

CAN WE TRUST SECURITY RATINGS?

Use and credibility of third-party security vendor security ratings

Shunsuke Koyama*

Abstract

This paper explores the questions about whether we can trust security ratings and how we should use them. My approaches are, (1) describing traditional and currently used vendor evaluation methods such as questionnaire, interview, and site-visits, (2) introducing security ratings, including the merits of using security ratings, use cases, limitations, and (3) conducting interviews and using a questionnaire for cybersecurity experts. According to my research, security ratings are quick, cost-effective, and objective; but at the same time, have limitations that security ratings are based on publicly available information and do not consider internal security measures. Due to such a feature, however, security ratings give us a quick view of the security posture of a vendor and tell us whether we should do further due diligence on what aspect. Therefore, I conclude that the security shall be used as a supplement to our vendor due diligence.

KEY WORDS: Computer Security; Cybersecurity; Security Ratings; Security Score; Vendor Assessment; Risk Assessment

* Brown University, Executive Master in Cybersecurity, expected in May 2020.

1. Problem We Face in Assessing Third-party Vendors

Working with various third-party vendors is necessary for an organization in the current business world. The reasons vary, such as seeking expertise or reducing overall costs. For example, in the banking industry, a bank works with vendors for payments, clearing, settlements, custody, and other corporate functions such as human resources, legal, and information technology. A large company or government agency works with several thousand third-party vendors[1] [2]. As companies work with more and more vendors, the number of cybersecurity incidents caused by or attributed to vendors has increased. According to the Ponemon Institute, "59 percent of respondents [to their survey] confirm that their organizations experienced a data breach caused by one of their vendors" [3] and "23 percent of respondent[s] say their organizations experienced a breach caused by one of their N^{th} parties"[4] in 2018.

To avoid vendor-related cybersecurity incidents, how to evaluate and select a third-party vendor, and how to continuously monitor them are critical risk management issues for an organization. Also, in some industries, regulators are focusing on vendor management. For example, in the banking industry, a federal regulator, the Office of the Comptroller of the Currency (OCC), has issued the risk management guideline. OCC expects banks "to practice effective risk management regardless of whether the bank performs the activity internally or

---

[1] For example, the U.S. Department of Defense has 16,000 vendors.
Mary E. Shacklett, "DOD Steps Up Supply Chain Security Programs for Smaller Contractors," *FedTech*, April 19, 2019, https://fedtechmagazine.com/article/2019/04/dod-steps-supply-chain-security-programs-smaller-contractors

[2] According to research by Forrester, an organization work with more than 4,700 third-party partners on average, and for example, a global manufacture works with more than 500,000 third parties worldwide.
Nick Hayes and Trevor Lyness, "The Forrester New Wave™: Cybersecurity Risk Rating Solutions, Q4 2018," *Forrester.com*, November 13, 2018,
https://www.forrester.com/report/The+Forrester+New+Wave+Cybersecurity+Risk+Rating+Solutions+Q4+2018/-/E-RES142874

[3] Ponemon Institute, *Data Risk in the Third-Party Ecosystem Third Annual Report* (Ponemon Institute, LLC, 2018), 7

[4] Ibid.

through a third party"[5]. Furthermore, OCC expects banks to conduct "periodic independent reviews" to assess whether the process aligns with the bank's strategy and effectively manages risk posed by third-party relationships[6].

This paper will describe the methods traditional and presently used by organizations to evaluate vendors, introduce three recent methods (standardized questionnaire, certification, and security ratings), and then pick up security ratings among them. The main questions to be discussed in this paper are "can we trust third-party security vendor security ratings," and "how should we use security ratings."

2. How to Evaluate Third-party Vendors?

2-1. Traditional Methods: Questionnaire, Interview, and Site-visit

Traditional methods to evaluate third-party vendors are the use of security questionnaires as well as interviews and site-visits. By using a questionnaire, organizations can get detailed written explanations of a vendor's security management program or policies. With Interviews, they can get information that is more relevant and probing, and not easy to write down or may not be public. They can also dive deeper into their concerns through discussion. Through site-visits, they can get various information not shown in the questionnaires or during interviews, including information regarding physical security. They can also verify information on their own.

However, there are three significant challenges with using traditional methods. First, questionnaires are subjective and not based on quantitative analysis[7]. Due to its technical nature,

---

5 Office of the Comptroller of the Currency, "Third-Party Relationships: Risk Management Guidance," OCC Bulletin 2013-29, October 30, 2013, https://www.occ.gov/news-issuances/bulletins/2013/bulletin-2013-29.html

6 Ibid.

7 Steve Zurier, "The security ratings game grades third-party vendors," *TechTarget*, September 1, 2016, https://searchsecurity.techtarget.com/feature/The-security-ratings-game-grades-third-party-vendors

describing security features is difficult, and an organization cannot compare several responses from vendors piece by piece. Second, questionnaires generally have too many questions[8] and is too time-consuming for third-party vendor' staff[9] [10]. Third, questionnaires, interviews, and site-visits are point-in-time snapshots of the security posture of the vendor, which show the third-parties' situation at a specific time. Organizations cannot conduct real-time monitoring of their vendors using these traditional methods.

2-2. Recent Methods: Standard Questionnaire, Certificate and Security Ratings

To overcome these challenges, organizations have three major solutions. The first is a standard questionnaire, which means that several organizations collectively prepare, or an industrial group prepares, a standard questionnaire. This standard questionnaire captures well-established security principles that most organizations will find meaningful to avoid duplicated questions from various organizations. For example, Shared Assessments provides a standardized questionnaire that can be used for various organizations to evaluate third-party vendors[11], which will save time for third-party vendors to respond to the questionnaires and also for organizations (users) to prepare the questionnaire and to check and analyze the responses. As another example, several U.S. financial institutions set up TruSight Solutions, LLC, which "combines best

---

[8] According to a study by a security rating provider, RiskRecon, the numbers of questions are about 280 in the finance and insurance industry, and about 190 in the health care industry.

RiskRecon, Inc. *Third-Party Security Risk Management Playbook 2018* (RiskRecon, Inc., 2018), 8.

[9] "The usual way of collecting vendor information is via a due diligence, a process that costs hours of work of highly trained staff and hours of the vendor's time."

Kenneth G. Crowther, Yacov Y. Haimes, and Eric M. Johnson, "Principles for Better Information Security through More Accurate, Transparent Risk Scoring," *Journal of Homeland Security and Emergency Management*: Vol. 7: Iss. 1, Article 37. (2010), 14.

[10] O'Malley and Hayes mention that "questionnaire practices are burdensome and error-prone."

Claire O'Malley and Nick Hayes, "Vendor Landscape: Third-Party Risk Intelligence," *Forrester.com*, October 20, 2017, 2, https://www.forrester.com/report/Vendor+Landscape+ThirdParty+Risk+Intelligence/-/E-RES131941

[11] "Standardized Information Gathering (SIG) questionnaire," The Santa Fe Group | Shared Assessments, accessed March 29, 2020, https://sharedassessments.org/sig/

practices and standardization to deliver comprehensive third-party risk assessment services"[12]. They gather and verify third-party's responses to their questionnaires and conduct remote assessments and onsite assessments. Such standardization and shared services are useful; however, they are still a snapshot of the security posture of the vendor during the time of the assessment.

The second solution is a certification. A certification shows that a third-party vendor meets and maintains a certain standard or requirements and should be qualified as a third-party vendor for an organization. For example, many organizations use the ISO Certification[13]. They obtain the ISO Certification to add credibility by reassuring counter-parities that they follow the ISO Standards[14]. Furthermore, the U.S. Department of Defense intends to introduce a certification[15] to be issued by an independent third-party assessment organization[16]. Checking whether a third-party vendor has a certification is easy for an organization, but on the other hand, maintaining the certification is generally costly for third-party vendors. Moreover, even though certificate holders should be reviewed periodically, it is still not real-time monitoring.

The third solution is using security ratings, which this paper is focused on below.

3. Security Ratings

3-1. What are Security Ratings?

---

12 "The New Industry Standard for Third-Party Risk," TruSight Solutions, LLC, accessed March 29, 2020, https://trusightsolutions.com/about

13 "Certification," International Organization for Standardization (ISO), accessed March 29, 2020, https://www.iso.org/certification.html

14 "ISO/IEC 27001 Information Security Management," ISO, https://www.iso.org/isoiec-27001-information-security.html

15 It is called Cybersecurity Maturity Model Certification.

16 "FAQ, Question 13," U.S. Department of Defense, accessed March 29, 2020, https://www.acq.osd.mil/cmmc/faq.html

Security ratings are quantifiable scores calculated by proprietary algorithms based on data points collected or purchased from public and private sources[17] [18] [19]. Gartner, a leading research and advisory company, "recognized an uptick in interest in SRS [security rating services]. Over the next five years [from 2018], these services will become a precondition for business relationships and part of the standard of due care for providers and procurers of services"[20]. As of this writing (March 2020), I could not find objective data regarding how many U.S. organizations use security ratings.

A security rating is based on the idea "that of bridging asymmetric information for a fraction of the cost of obtaining information"[21]. While a rated organization knows well their internal security structure, others do not know it. Therefore, paying to the fraction of cost, they obtain the ratings so that they can understand the external posture of the rated organization. This is similar to a credit score for an individual[22] or a credit rating for an organization[23].

---

[17] U.S. Chambers of Commerce explains "security rating companies 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."

"Principles for Fair and Accurate Security Ratings," U.S. Chambers of Commerce, June 20, 2017, https://www.uschamber.com/issue-brief/principles-fair-and-accurate-security-ratings

[18] Olyaei, et al. explain "security rating services provide continuous, independent and quantitative technical analysis and scoring for public-facing digital assets of organizational entities across geographies."

Sam Olyaei, Christopher Ambrose, and Jeffrey Wheatman, "Innovation Insight for Security Rating Services," *Gartner.com*, Refreshed September 10, 2019; Published July 27, 2018, https://www.gartner.com/en/documents/3884271/innovation-insight-for-security-rating-services

[19] BitSight explains security ratings as follows: "security ratings are a data-driven, dynamic measurement of an organization's cybersecurity performance. Ratings are derived from objective, verifiable information and created by independent organizations."

BitSight Technologies, "Security Ratings Explained," accessed March 29, 2020, https://info.bitsight.com/cybersecurity-101-security-ratings-explained

[20] Olyaei, Ambrose, and Wheatman, "Innovation Insight for Security Rating Services."

[21] Eric Johnson, and Igor Macura, "Information Risk and the Evolution of the Security Rating Industry," *Tuck School of Business, Dartmouth College*, March 24, 2009.

[22] Credit score is a number that shows individual's creditworthiness. Equifax, Inc., one of the three major credit bureaus, explains "credit scores are calculated using information in your credit report, including your payment history; the amount of debt you have; and the length of your credit history."

Equifax, Inc, "What is the Good Credit Score," accessed March 29, 2020, https://www.equifax.com/personal/education/credit/score/what-is-a-good-credit-score/

[23] Regarding credit ratings, Moody's explains "ratings assigned on Moody's global long-term and short-term rating scales are forward-looking opinions of the relative credit risks of financial obligations issued by non-financial corporates, financial institutions, structured finance vehicles, project finance vehicles, and public sector entities."

Below, this paper analyzes how organizations can use security ratings as a part of security risk management, what the advantages or merits of using security ratings are, and what the limitation of security ratings are. Then, this paper introduces the research results regarding how companies are using security ratings. Finally, this paper proposes how an organization should use security ratings and what security ratings should be in the near future.

3-2. Merits or Advantages of Using Security Ratings

According to security rating providers, there are several merits or advantages of using security ratings.

(1) Quick and Continuous Monitoring

Security ratings enable users to monitor vendors in real-time. Security ratings will change periodically once rating providers notice any changes in data points. Such periodical change is a critical factor for security ratings that differentiate from other evaluation methods such as questionnaires or interviews.

(2) Objective and Comparable

Security ratings are objective, and users of security ratings can compare ratings of rated organizations. Security rating providers do not use any inputs from a human; instead, calculate the ratings using their algorithms and combining available data. Furthermore, they collect the same scope of data and use the same algorithms for various organizations to be rated; as a result, a user can compare the security ratings of rated organizations with the ratings of its competitors or its peers calculated by the same rating provider.

(3) Easily Reachable to 4^{th}, 5^{th} or N^{th} Parties

Moody's Investor Services, Inc., *Rating Symbols and Definitions* (Moody's Investor Services, Inc., January 2020), 5

In the current business world, it is common for an organizations' third party to work with other organizations, which are 4th, 5th, or Nth parties for the original organization. The original organization easily grasp the external security exposure of 4th, 5th, or Nth parties by using security ratings.

(4) Saving Cost

Security ratings could save cost for users because users can reduce the time for their due diligence and focus on low security rating vendors. Using security ratings itself incurs costs (e.g., license or subscription fee); however, security rating providers do not conduct any costly investigation such as penetration tests or site-visits. Therefore, overall cost for users would be lower[24].

3-3. Use Cases for Security Ratings

Security ratings will be useful for the following cases[25].

(1) Vendor Evaluation

Evaluating vendors is the original purpose of security ratings. Organizations can seek the ratings of their vendors or partners to evaluate potential risks related to the vendors or partners[26]

---

[24] According to a research by Forrester (commissioned by Security Scorecard), a user of security ratings could save several million USD for each of increase of productivity in the vendor risk management security and account teams ($3.2 million), avoidance [or reduction] of outside consulting fees ($1.8 million), improvement in efficiency in vendor procurement and onboarding ($1.6 million), and improvement in business process of vendor risk assessment ($1.2 million) for three years. The estimate is based on the Forrester's four customers.

Forrester Research Inc., *The Total Economic Impact™ of Security Scorecard* (Forrester Research Inc., March 2019), 3.

[25] BitSight explains "businesses use these ratings to screen and monitor third parties, underwrite cyber insurance coverage, monitor investment portfolios, benchmark their own security programs and more."

BitSight Technologies, *How BitSight Calculates Security Ratings* (technical note) (BitSight Technologies), 1.

[26] Ann M. Beauchesne, "Why We Need Fair and Accurate Cybersecurity Ratings," *U.S. Chamber of Commerce*, June 20, 2017, https://www.uschamber.com/series/above-the-fold/why-we-need-fair-and-accurate-cybersecurity-ratings

[27]. At the same time, some organizations show the security rating of a vendor to the vendor and discuss how to improve the vendor's cybersecurity exposure[28].

2) Self-evaluation - Improvement

Checking their own ratings, organizations can identify weaknesses in their security programs or see how they rank against competitors[29] [30] [31].

3) Self-evaluation - Marketing

Showing their security rating, vendors can demonstrate their good security posture to their counter-parties, and help "their customers more efficiently and effectively manage their own third-party risks."[32] If a vendor's ratings is improved, the vendor may be subject to "lighter reviews" [33] by their counter-parties during their due diligence in the future.

4) Cybersecurity Insurance

Insurance providers can use security ratings into their cybersecurity insurance underwiring calculations[34] [35]. The cybersecurity insurance industry lacks common or standard

---

[27] Olyaei, Ambrose, and Wheatman, "Innovation Insight for Security Rating Services."

[28] A research commissioned by BitSight shows that "43% of companies using cybersecurity ratings also report them out to customers and partners."
Forrester Research Inc., *Better Security and Business Outcomes with Security Performance Management* (Forrester Research Inc., September 2019), 4.

[29] Beauchesne, "Why We Need Fair and Accurate Cybersecurity Ratings."

[30] Olyaei, et al. explain that organizations can "compare their posture with that of their peers or competitors."
Olyaei, Ambrose, and Wheatman, "Innovation Insight for Security Rating Services."

[31] BitSight explains that security ratings "provide comparative analysis to benchmark data breach risk among industry peers. Remediate issues with detailed forensics to lower your risk of a breach."
BitSight Technologies, *BitSight Security Ratings Correlate to Breaches* (BitSight Technologies), 1.

[32] Olyaei, Ambrose, and Wheatman, "Innovation Insight for Security Rating Services."

[33] Security Scorecard, *The Expanding Role of Security Ratings* (Featuring Research from Forrester) (Security Scorecard, 2018), 8.

[34] FICO mentions "as cyber insurance is a relatively new class of insurance, underwriters have lacked historic actuarial data upon which to base underwriting decisions. The FICO Enterprise Security Score provides an accurate, empirical, and forward-looking assessment of the overall cyber risk exposure of an enterprise, which insurers can use for underwriting, pricing and ongoing portfolio management."
Fair Isaac Corporation, "Barbican Insurance Group Partners with FICO to Enhance Cyber Underwriting, *FICO*, January 17, 2018, https://www.fico.com/en/newsroom/barbican-insurance-group-partners-fico-enhance-cyber-underwriting

[35] Olyaei, Ambrose, and Wheatman, "Innovation Insight for Security Rating Services."

metrics to evaluate risks[36]. Using security ratings, they can initially and continuously evaluate the security posture of current and future customers[37].

5) Merger and Acquisitions

A potential buyer in an M&A transaction can use the security ratings to check or monitor the security posture of a target[38]. Even if the target's security exposure is not accessible or available, the buyer can get the score and quickly decide whether they need in-depth due diligence or not.

3-4. Limitations of Security Ratings

On the other hand, there are several limitations of security ratings.

(1) Inside Activities - Not Considered

Security rating providers only collect and use public information or externally available information. They do not conduct penetration tests and consider a perspective of internally layered control that would protect an organization. In practice, many organizations adopt a layered approach such as network segmentation and conduct employee training to strengthen the security of the organization. However, security rating providers do not consider these efforts at all[39].

(2) Accurate Scanning of IP Address

Security ratings "depends on the ability of the rating provider to accurately attribute the scanned Internet Protocol (IP) addresses to an individual organization"[40]. In practice, some IPs

---

36 Zurier, "The security ratings game grades third-party vendors."
37 Olyaei, Ambrose, and Wheatman, "Innovation Insight for Security Rating Services."
38 BitSight Technologies, *BitSight Security Ratings Correlate to Breaches*.
39 For rated organizations, such efforts are sensitive information. Rated organizations "strive to minimize the risk of their weaknesses being exploited." Crowther, Haimes, and Johnson, "Principles for Better Information Security through More Accurate, Transparent Risk Scoring," 14.
40 American Bankers Association, *Security Ratings: A Tool as Part of a Risk Management Program* (American Bankers Association, August 2019), 2.

associated with an organization, and included in the security ratings, may not belong to that organization. In contrast, others that belong to an organization may not be included"[41] due to its intricate network structure. Therefore, the basis of security ratings might be questionable.

(3) No Standardized Evaluation Methods

The security rating industry is new and still in the developing phase. Many security rating providers are competing, and no standardized evaluation methods or no market-agreed methods exist[42] [43]. As a result, a rated organization may be rated differently in several rating providers.

4. Research

To understand what cybersecurity experts view security ratings, I conducted interviews and collected questionnaires from information security professionals.

4-1. Interview

I joined an information security professionals' meeting in Boston in October 2019 and discussed how they use the security ratings. The followings are their thoughts on security ratings.

- Professional A: I am using a security rating provider. Their score is supplement to our own due diligence.
- Professional B: I think security rating providers are not well trusted. I obtained a report of my company from a security rating provider, but I found it was not accurate. The reason was that they only collected public information. I also heard

---

41 Ibid.

42 Gartner mentions that "no single service or solution has yet matured enough to provide ratings that have been consistently time-tested."
Brian Reed, Neil MacDonald, Peter Firstbrook, Sam Olyaei, and Prateek Bhajanka, "Top 10 Security Projects for 2019," *Gartner.com*, February 11, 2019.

43 "No single service or solution has yet matured to provide ratings that have been consistently time-tested." Olyaei, Ambrose, and Wheatman, "Innovation Insight for Security Rating Services."

that if my company becomes their customer (subscriber), then our score would become better.[44]

4-2. Questionnaire

I asked several experts to answer a questionnaire that I developed[45]. Responses were anonymous. All respondents were cybersecurity professionals.

Followings are their thoughts on security ratings:

- A user does not rely on the security ratings solely, and instead, they use the ratings as a secondary reference to support their own evaluations.
- A non-user has a concern that their government counter-party would not allow them to use a third party for vendor evaluation.
- Another non-user also shares their concern about exposing their security posture. They do not want someone else to have non-public information about their security.
- Another non-user questions the validity of the ratings or reports provided by security rating providers because such ratings and reports are self-evaluation or report.

5. Analysis

5-1. Can We Trust Security Ratings?

(1) Ideal Security Ratings - Correlation to Breaches

The question "can we trust third-party vendor security ratings" relates to the use of security ratings. If an organization understands that the rating is an analysis of an external view of a rated organization and does not reflect any internal means to protect their assets, they can trust and use it as an external view combining with other evaluation tools. This is the value of security ratings.

---

44 Interview by an author, October 16, 2019.

45 The questionnaire and all replies are described in Exhibit 1 - Questionnaire.

At first, what are the use of security ratings? In other words, what do users want the ratings to be? Using security ratings is only a part of third-party risk management. Accordingly, the users want the security ratings to show the risk of a third party accurately, especially risks that the third party might cause a cybersecurity incident, such as data leakage. Therefore, ideal security ratings should inform users of the risk of cybersecurity incidents due to the third-party vendor.

Currently, several security rating providers show that their ratings correlate to breaches[46] [47]. Security ratings of each organization are not publicly available[48] due to the policies of security rating providers or "Principles for Fair and Accurate Security Ratings" established by U.S. Chambers of Commerce[49]. Therefore, I cannot independently verify any correlations between security ratings calculated by each security rating provider and disclosed data breaches of rated organizations. Such correlation, however, will become one of the good reasons why

---

[46] According to BitSight, their research "demonstrates that companies with higher ratings are less likely to have experienced a publicly disclosed data breach. Specifically, companies with a rating of 400 or lower were five times more likely to experience a publicly disclosed data breach than companies with a 700 or higher."

BitSight Technologies, *BitSight Security Ratings Correlate to Breaches*.

Note that BitSight's ratings "range from 250-900 with a higher rating indicating better security performance". BitSight Technologies, *How BitSight Calculates Security Ratings* (BitSight Technologies).

[47] According to the website of a security rating provider, FICO (Fair Isaac Corporation), "the model powering the FICO Enterprise Security Score now has a dynamic range of more than 24X, which means that the lowest scoring organizations have a breach risk 24 times higher than those with the highest scores. Our experience with AI and machine learning led directly to this huge improvement in performance."

Fair Isaac Corporation, "FICO Doubles the Power of Cybersecurity Score to Predict Breaches", *FICO*, October 11, 2017, https://www.fico.com/en/newsroom/fico-doubles-power-cybersecurity-score-predict-breaches

[48] Crowther, et al. mention that "a serious obstacle to the growth of the industry may be the fact that the ratings and the rating reports are confidential."

Crowther, Haimes, and Johnson, "Principles for Better Information Security through More Accurate, Transparent Risk Scoring," 15.

Eric and Igor mention "a serious obstacle to the growth of the industry may be the fact that the ratings and the rating reports are confidential."

Eric, and Igor, "Information Risk and the Evolution of the Security Rating Industry,"

[49] U.S. Chambers of Commerce published "Principles for Fair and Accurate Security Ratings" and several security ratings providers are supportive of the principles including but not limited to BitSight, FICO, RiskRecon and Security Scorecard. Confidentiality is one of the principles.

U.S. Chambers of Commerce, "Principles for Fair and Accurate Security Ratings."

The principle is attached as Exhibit 3.

organizations should use the security ratings. According to a security rating provider, several security rating providers scored Equifax as a high risk to suffer a data breach several months before it announced its massive data breach in the summer 2017[50]. This is an example of how security ratings should work. Nonetheless, being able to provide information to users about a third-party's risk of a data breach is an important finding for an organization's vendor management program.

(2) Factors to be Considered

Each security rating provider discloses what data they collect and use to calculate their security ratings[51]. It is difficult to compare or analyze one by one because each security rating provider categorizes data differently. Overall, they use all or some of the followings: (1) compromised systems, (2) organization's actions to secure their system or to prevent data breach, (3) users' behavior, (4) publicly disclosed breach information, and (5) threat intelligence or information from Dark Web.

5-2. How Should We Use Security Ratings?

As mentioned above, security ratings have both merits or advantages and limitations. Security ratings "represent an encapsulation of available data points and may not reflect nuances and effective security controls layered within a rated organization's security program."[52] Therefore, we should use security ratings with an understanding of what they are and what they are not. Security ratings will be beneficial to organizations not as the full answer, but as another tool to use to evaluate third-party vendors.

(1) Supplement

---

50 Security Scorecard, *The Expanding Role of Security Ratings (Featuring Research from Forrester),* 8.
51 Exhibit 2 shows what data each security rating provider considers.
52 Beauchesne, "Why We Need Fair and Accurate Cybersecurity Ratings."

Security ratings shall be used as "supplement" to other evaluation tools. Organization's own assessment other than security ratings is assumption or pre-requisite, and user organizations cannot solely rely on the security ratings.

Security ratings are based on public-facing assets and are not a whole picture of the security posture of a rated organization. A criticism against security ratings is that the rating providers should consider the rated organization's effort, such as layered control. To discuss whether the rating providers should consider such internal information, let us assume a case if a security rating reflects all security posture of a rated organization. First, security rating providers would need internal security information of a rated organization. Some organizations would be cooperative and provide such internal information, but others would not because such internal information is sensitive and should not be disclosed. Therefore, security ratings would not cover all organizations but some limited number of organizations. Furthermore, security ratings might reveal the vulnerabilities of a rated organization, which is not public. Such vulnerabilities would be valuable information for potential attackers. Besides, since security rating providers would store such precious internal information, they might become the targets of potential attacks. Also, if security rating providers collect internal information or conduct penetration tests, they cannot provide ratings quickly, and their cost will increase. One of the merits of current security ratings is quick and low cost. Therefore, if a security rating reflects all security posture of a rated organization, that would diminish the merits of the current security ratings[53].

---

[53] Rather, there are several merits coming from the fact where security ratings are not a whole picture but based on the Internet faced information. For example, security rating providers can access to data to be used for their ratings independently and remotely without any assistance by rated organizations; therefore, they can calculate the ratings for any organization anytime. If anything in the data that a security rating provider is monitoring changes, the provider can adjust the ratings immediately. Therefore, users can get real-time security ratings of the rated organizations.

UpGuard, Inc., *The Buyer's Guide to Third Party Risk Management* (UpGuard Inc., 2019), 3.

(2) Are There Any Advantages of Using Security Ratings Even If They Are Not a Whole Picture?

Even if security ratings are not a whole picture of the security exposure of an organization, there are still advantages to using them as follows.

(i) Initial Phase - Vendor Selection Phase

Depending on a security rating of a third-party vendor, an organization can change the level or depth of due diligence of third-party vendors. For example, they can choose a “light” due diligence if a third-party vendor that has an excellent score from a security rating provider. In contrast, they can choose deep due diligence if a third-party vendor has a lower rating than its peers. Also, if a third-party vendor has a lower score than its peers, it will trigger the need to investigate the vendor’s security posture in a more in-depth way and to find out why their rating is low. At a minimum, the security rating tells the users whether a third-party vendor is high-risk. Using security ratings in the initial phase, a user organization could quickly understand the security feature of a vendor and prioritize which third-party vendors they should conduct in-depth due diligence.

At the same time, security rating users can focus on concerns related to internal security means when they use a questionnaire or conduct interviews because such means are not reflected in the security ratings.

(ii) Monitoring Phase

Real-time monitoring (or active monitoring) is one of the advantages of using security ratings. If a user confirms a change in a vendor’s score, it may mean that there is a change in the vendor’s publicly faced exposure. If the change is a significant negative one, it will trigger a

more in-depth investigation into the vendor's security posture[54]. This is significant merit of using security ratings because they can be updated periodically (almost daily)[55]. In any case above, it is clear that the security ratings should be used as a supplement to the due diligence that organizations are performing on their third-party vendors.

(3) What Security Ratings Should Be in the Near Future

Security rating providers should be verified by independent organizations. Disclosing the details of rate calculation or its algorithms is difficult for security rating providers because such calculation methods or algorithms are the core values of the providers. From the users' perspective, however, they cannot trust a black box or secret algorithms. Therefore, security rating providers should be examined, and their calculation methods and algorithms should be validated by independent organizations so that independent organizations should ensure the rating providers' calculation methods and algorithms are rational and reliable.

6. Conclusion

While there are several limitations such as ratings are based on publicly available information, security ratings can work as a supplement to an organization's vendor management program. Security ratings will give users a quick image of the security posture of a vendor, provide them with information whether there is a change to the vendor's security, and can assist organizations to determine whether they need to conduct further due diligence and how deep the investigation should be. With understanding such features, we can trust and use security ratings.

---

[54] "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."

American Bankers Association, *Security Ratings: A Tool as Part of a Risk Management Program* (ABA, August 18, 2019), 5

[55] UpGuard mentions that "traditional business assessments follow traditional business cadences: annually, quarterly— but cyber risk changes daily, hourly, in real time as someone works on a system. Security ratings should continuously audit the vendors they score to always have a current risk analysis and to provide historical trends and timelines."

UpGuard, Inc., *The Buyer's Guide to Third Party Risk Management*, 3

Appendix

Exhibit 1: Questionnaire and Responses

For Users

Question 1: How are you using the security ratings to evaluate third party vendors?
- As a secondary reference to support our own evaluations

Question 2: Do you rely on security ratings?
- Not solely

Question 3: Do you do due diligence by yourself (security ratings are supplement?)
- Yes, we have a team that does this.

Question 4: After using security ratings, have you changed your third-party due diligence?
- No.

Question 5: Could you tell us what makes security ratings better?
- Better verification of the third-party data
- Fewer questions
- Greater transparency way to collect more accurate data

Question 6: What feature that security rating company provides do you find values in your third-party due diligence?
- A way to "normalize" ratings across most vendors

For Non-Users

Question: Could you tell us why you do not use it? What is your concern?
- We do our own due diligence. No third party at all. The concern is that we would be exposing our security posture.
- Also, our government counter-party would not let us use a third party for this.
- We do not see the value. In addition, it is another third-party risk. In other words, we will not want someone else going in our "inside the box".
- The ones I have seen are self-assessment, so I question the validity of the report. Also, if one person responds, the person may not have sufficient knowledge to answer all questions.

Exhibit 2: What data each security rating provider considers

1. BitSight Technologies

BitSight Technologies is a pioneer in the security ratings industry. Their customer is over 1,800, and they calculate security ratings for more than 170,000 organizations[56].

BitSight discloses the following four data categories in their security rating platform.

> (1) Compromised Systems
> Compromised Systems are devices within an organization's network that are infected with malware.
>
> (2) Diligence
> Diligence records demonstrate the steps a company has taken to prevent attacks.
>
> (3) User Behavior
> User Behavior examines activities that may introduce malicious software onto a corporate network, for example, by downloading a compromised file.
>
> (4) Public Disclosures
> BitSight collects information about publicly disclosed breaches and interruptions to business continuity from a variety of news sources and data breach aggregation services. A breach is attributed to a company when there is significant, publicly-disclosed evidence that the company was at fault for the data loss, such as a company-issued disclosure notice or investigation from a credit card company.[57]

---

[56] BitSight Technologies, "Why BitSight?" https://www.bitsight.com/why
[57] BitSight Technologies, "BitSight Data," https://www.bitsight.com/data

2. Security Scorecard

Security Scorecard, Inc. is one of the market leaders in the security rating industry and "was one of the first to market with its cyber-risk rating tool"[58]. They use the following risk factors to calculate security ratings.

(1) Network Security
Examples of network security hacks include exploiting vulnerabilities such as open access points, insecure or misconfigured SSL certificates, or database vulnerabilities and security holes that can stem from the lack of proper security measures.

(2) DNS Health
The Security Scorecard platform measures multiple DNS configuration settings, such as OpenResolver configurations as well as the presence of recommended configurations such as DNSSEC, SPF, DKIM, and DMARC.

(3) Patching Cadence
How diligently a company is patching its operating systems, services, applications, software, and hardware in a timely manner.

(4) Endpoint Security
Endpoint security refers to the protection involved regarding an organization's laptops, desktops, mobile devices, and all employee devices that access that company's network.

(5) IP Reputation
The Security Scorecard sinkhole system ingests millions of malware signals from commandeered Command and Control (C2) infrastructures from all over the world. The incoming infected IP addresses are then processed and attributed to corporate enterprises through our IP attribution algorithm. The quantity and duration of malware infections are used as the determining factor for these calculations, providing a data point for the overall assessment of an organization's IP Reputation, along with other assessment techniques.

(6) Web Application Security
Examples of vulnerabilities detected include Cross-site Scripting (XSS) or an SQL injection attacks.

(7) Cubit Score
The Cubit Score factor is Security Scorecard's proprietary threat indicator that measures a collection of critical security and configuration issues related to exposed administrative portals.

---

[58] Hayes and Lyness, "The Forrester New Wave™: Cybersecurity Risk Rating Solutions, Q4 2018", 10.

(8) Hacker Chatter

The Security Scorecard Hacker Chatter factor continuously collects communications from multiple streams of underground chatter, including hard-to-access or private hacker forums. Organizations and IPs that are discussed or targeted are identified.

(9) Leaked Credentials

Security Scorecard identifies all sensitive information that is exposed as part of a data breach or leak, keylogger dumps, paste bin dumps, database dumps, and via other information repositories. Security Scorecard maps the information back to the companies who own the data or associated email accounts that are connected to the leaked information, assessing the likelihood that an organization will succumb to a security incident due to the leaked information.

(10) Social Engineering

Security Scorecard identifies a variety of factors related to social engineering, such as employees using their corporate account information for services, for example, social networks, service accounts, personal finance accounts, and marketing lists that can be exploited. In addition, employee dissatisfaction is monitored through publicly available data. [59]

[59] Security Scorecard, Inc., "Security Ratings / It all starts a score," https://securityscorecard.com/platform/security-ratings

Exhibit 3: Principles for Fair and Accurate Security Ratings[60]

Principles for Fair and Accurate Security Ratings

As security ratings continue to mature, more organizations in the public and private sectors leverage them in making business and risk decisions. As a key piece of a robust security evaluation program, security ratings based on accurate and relevant information are useful tools in evaluating cyber risk and facilitating collaborative, risk-based conversations between organizations. Security rating companies 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 upon the quality and breadth of the data they use, the variety of sources and the dynamic nature of the environment create risks of producing ratings that can potentially be inaccurate, irrelevant or incomplete. To increase confidence in security ratings, an industry-wide, common approach should:

- Promote quality and accuracy in the production of security ratings
- Promote fairness in reporting
- Include a coordinated process for adjudicating errors or inaccuracies in reported content
- Establish guidelines for appropriate use and disclosure of the scores and ratings

We believe these principles will promote fairness in reporting and enhance the value of security ratings across all industries.

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 companies 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 companies shall provide reasonable notice to their customers and clearly communicate how announced changes may impact existing ratings.

Independence: Commercial agreements, or the lack thereof, with rating companies shall not have direct impact on an organization's rating; any rated organization will be able to

60 US Chambers of Commerce, "Principles for Fair and Accurate Security Ratings."

see and challenge their rating irrespective of whether they are a customer of the rating company.

Confidentiality: Information disclosed by a rated organization during the course of a challenged rating or dispute shall be appropriately protected. Rating companies should not publicize an individual organization's rating. Rating companies shall not provide third parties with sensitive or confidential information on rated organizations that could lead directly to system compromise.

Bibliography

American Bankers Association. *Security Ratings: A Tool as Part of a Risk Management Program*. ABA, August 2019.

Beauchesne, Ann M. "Why We Need Fair and Accurate Cybersecurity Ratings." *U.S. Chamber of Commerce*, June 20, 2017. https://www.uschamber.com/series/above-the-fold/why-we-need-fair-and-accurate-cybersecurity-ratings

BitSight Technologies. *BitSight Security Ratings Correlate to Breaches.*

BitSight Technologies. *How BitSight Calculates Security Ratings (technical note).*

BitSight Technologies. "Why BitSight?" https://www.bitsight.com/why

BitSight Technologies. "BitSight Data" https://www.bitsight.com/data

BitSight Technologies. "Security Ratings Explained." Accessed March 29, 2020. https://info.bitsight.com/cybersecurity-101-security-ratings-explained

Crowther, Kenneth G., Yacov Y. Haimes, and Eric M. Johnson. "Principles for Better Information Security through More Accurate, Transparent Risk Scoring." *Journal of Homeland Security and Emergency Management*: Vol. 7: Iss. 1. Article 37. (2010).

Equifax, Inc. "What is the Good Credit Score." Accessed March 29, 2020. https://www.equifax.com/personal/education/credit/score/what-is-a-good-credit-score/

Fair Isaac Corporation. "Barbican Insurance Group Partners with FICO to Enhance Cyber Underwriting." *FICO*, January 17, 2008. https://www.fico.com/en/newsroom/barbican-insurance-group-partners-fico-enhance-cyber-underwriting

Fair Isaac Corporation. "FICO Doubles the Power of Cybersecurity Score to Predict Breaches." *FICO*, October 11, 2017. https://www.fico.com/en/newsroom/fico-doubles-power-cybersecurity-score-predict-breaches

Forrester Research Inc. *Better Security and Business Outcomes with Security Performance Management*. Forrester Research Inc., September 2019.

Forrester Research Inc. *The Total Economic Impact™ of Security Scorecard*. Forrester Research Inc., March 2019.

Hayes, Nick, and Trevor Lyness. "The Forrester New Wave™: Cybersecurity Risk Rating Solutions, Q4 2018." *Forrester.com*, November 13, 2018. https://www.forrester.com/report/The+Forrester+New+Wave+Cybersecurity+Risk+Rating+Solutions+Q4+2018/-/E-RES142874

International Organization for Standardization (ISO). "Certification." Accessed March 29, 2020. https://www.iso.org/certification.html

International Organization for Standardization (ISO). "ISO/IEC 27001 Information Security Management." Accessed March 29, 2020. https://www.iso.org/isoiec-27001-information-security.html

Johnson, Eric, and Igor Macura. "Information Risk and the Evolution of the Security Rating Industry." *Tuck School of Business, Dartmouth College*, March 24, 2009.

Moody's Investor Services, Inc. *Rating Symbols and Definitions.* January 2020.

Office of the Comptroller of the Currency. "Third-Party Relationships: Risk Management Guidance." OCC Bulletin 2013-29. October 30, 2013. https://www.occ.gov/news-issuances/bulletins/2013/bulletin-2013-29.html

Olyaei, Sam, Christopher Ambrose, and Jeffrey Wheatman. "Innovation Insight for Security Rating Services." *Gartner.com*, Refreshed September 10, 2019; Published July 27, 2018. https://www.gartner.com/en/documents/3884271/innovation-insight-for-security-rating-services

O'Malley, Claire, and Nick Hayes. "Vendor Landscape: Third-Party Risk Intelligence." *Forrester.com*, October 20, 2017. https://www.forrester.com/report/Vendor+Landscape+ThirdParty+Risk+Intelligence/-/E-RES131941

Ponemon Institute, LLC. *Data Risk in the Third-Party Ecosystem Third Annual Report*. Ponemon Institute, LLC, 2018.

Reed, Brian, Neil MacDonald, Peter Firstbrook, Sam Olyaei, and Prateek Bhajanka. "Top 10 Security Projects for 2019." *Gartner.com*, February 11, 2019.

RiskRecon, Inc. *Third-Party Security Risk Management Playbook 2018*. RiskRecon, Inc., 2018.

The Santa Fe Group | Shared Assessments. "Standardized Information Gathering (SIG) questionnaire." Accessed March 29, 2020. https://sharedassessments.org/sig/

Security Scorecard. *The Expanding Role of Security Ratings (Featuring Research from Forrester).* Security Scorecard, 2018.

Shacklett, Mary E. "DOD Steps Up Supply Chain Security Programs for Smaller Contractors." *FedTech*, April 19, 2019. https://fedtechmagazine.com/article/2019/04/dod-steps-supply-chain-security-programs-smaller-contractors

TruSight Solutions, LLC. "The New Industry Standard for Third-Party Risk." Accessed March 29, 2020, https://trusightsolutions.com/about

UpGuard, Inc. *The Buyer's Guide to Third Party Risk Management*. UpGuard Inc., 2019.

U.S. Chambers of Commerce. "Principles for Fair and Accurate Security Ratings." June 20, 2017 https://www.uschamber.com/issue-brief/principles-fair-and-accurate-security-ratings

U.S. Department of Defense. *FAQ, Question 13*. Accessed March 29, 2020. https://www.acq.osd.mil/cmmc/faq.html

Zurier, Steve. “The security ratings game grades third-party vendors.” *TechTarget*, September 1, 2016. https://searchsecurity.techtarget.com/feature/The-security-ratings-game-grades-third-party-vendors