CSW Cyber SecurityWorks

Whitepaper


# Security Ratings- Quantifying Cyber Risk Exposure

Abstract— Most companies today manage security risk as part of their overall IT practice, which is based on checklist or point-in-time approach. While it is difficult to quantify security efforts and determine where to apply resources, there are few objective metrics that enable a company to measure its security posture continuously and evaluate whether it has improved or worsened. The purpose of this study is to analyze the cyber risk exposure of an organization and quantify the risk against industry. Security rating approach has been used to calculate the score, which gives an insight of each risk in detail. The proposed risk rating helps the organization to know their cyber risk and implement the countermeasures to mitigate and improve cyber posture on a continuous basis.

Keywords—security rating, risk exposure, cyber posture

## I. INTRODUCTION

Most companies today manage security risk as part of their overall IT practice, often without much interaction from other parts of the business. They purchase products such as firewalls, intrusion detection systems, and security information and event management (SIEM) tools to help protect their organization. They set internal policies with employees and help educate them on how to protect themselves and the organization from phishing attacks. They spend time and resources ensuring they have all of the appropriate industry certifications and that they are meeting global or industry compliance requirements, such as HIPAA, PCI, NIST, or GDPR.

While it is difficult to measure the efficacy of security spend and determine where to apply resources, there are few objective metrics that enable a company to measure its security posture continuously, and evaluate whether it has improved or worsened. Thus, security spending increases globally year after year in an attempt to mitigate risk as the frequency of cyber-attacks is on the rise. It also is difficult to gain insight into third-party risk. Leading security groups attempt to measure the IT security posture of third parties by collecting information through a requirements checklist or questionnaire, or by getting their organisation attested by an auditor to attain industry required compliance. These standards can provide a good indicator of where to utilize resources, as well as where to start a third-party evaluation.

## II. THE PROBLEM

Using these methods alone to assess security risk, though, is not sufficient. This is proven by the growing number of public breaches that involve business partners.

The dynamic nature of cyber risk is so, that no amount of audit or however complete the checklists are, the results reflect only for that moment. Though

penetration scans or vulnerability test are conducted, its results may not be valid the following week.

These types of risk assessments are old school and cannot scale to keep up with rapidly growing businesses and their subsequent cybersecurity programs. For organisations to be proactive and avoid risks in their cyber ecosystem, they need to be evaluating their security posture by gaining insight into their flaws of the network and all assessments need to be heavily data oriented and evidence based providing them with issues and mitigating plans that regular audits cannot foresee.

Complementing a security assessment with the continuous evaluation of security effectiveness allows organizations to augment their view into the security risks of the extended enterprise. In addition to gaining visibility into the weaknesses of a network, a data-driven, evidence-based assessment can allow organizations to mitigate new risks proactively as they emerge and identify issues that a regulatory audit was not designed to catch.

By taking these steps, organizations can move toward a mature, risk based security program and away from the simpler checkbox, point in-time model.

## III. SECURITY RATING – NEW APPROACH

A security rating is a more efficient and effective cyber risk management driven by organisational cyber data and dynamic and aggressive measurement of an organization's general security posture

For security professionals, security ratings provide a clear picture of the security posture of their own organizations and their third-party as well.

### A. Risk Rating Approach

Security Ratings measure the security posture of organizations. These ratings can have any measurable range (In this paper we are using 300-850 with a higher rating indicating better security posture). All data collected are normally externally visible using passive reconnaissance. This means that no active reconnaissance are performed like

penetration tests or vulnerability scans on any organization in order to collect information. The calculation of risk ratings, should be based on diversified data collected from different source like surface web, deep web and dark web - ensuring that customers gets the most accurate security ratings. The collected data is processed using customized and flexible algorithms.

### B. Extensive Coverage of Attack Surface

Data should be collected for different facets to ensure entire IT landscape of an organization is covered and an organization receives most accurate security posture rating. All IP/assets belonging to an organization, together with the combination of installed OS, apps and/or data, constitute the attack surface. Data related to entire attack surface should be searched for security risks. In this paper we have categorized attack surface into five facets.

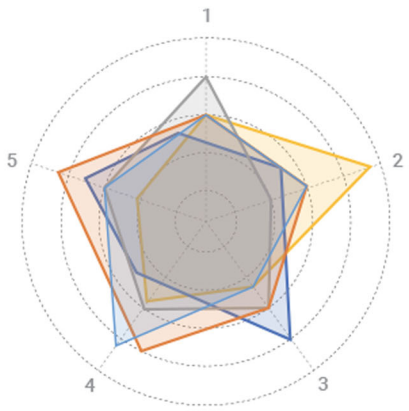


Fig. 1. Rating for entire attack surface of an organisation

Each facet is again analyzed in detailed and ratings are provided based on the risk calculated from the data gathered against each facet.

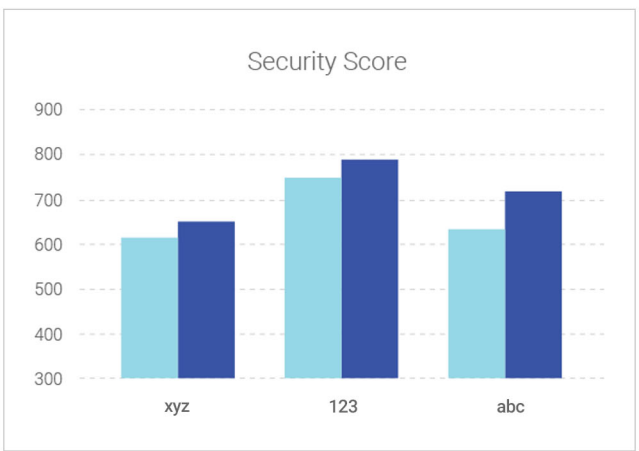


Fig. 2. Rating for individual facet

### C. Peer to peer rating comparision

The platform should also enable organization to compare their score with industry peer. This helps the organization in benchmarking its security posture against different industry and ultimately help them improve their score.

Platform should also provide organization with the ability to measure security posture of its vendor or other organization in its portfolio.

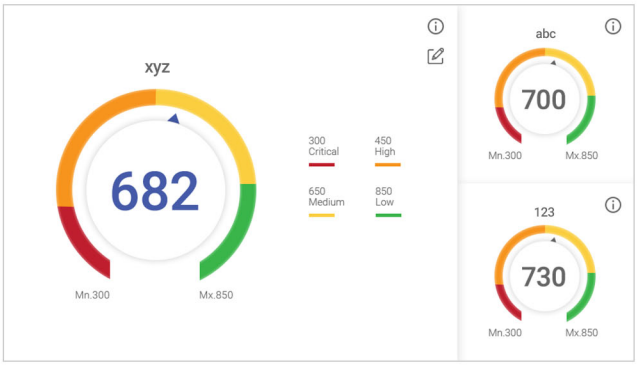


Fig. 3. Rating comparion with industry peer

D. Usage of security ratings

Security risk managers need data driven, objective, and comparable metrics to help them manage risk more effectively. Security ratings can create market efficiencies that lead to improved cybersecurity practices.

Security Ratings helps to manage cyber risk in the following ways:

- Security Posture Management
- Third-Party Risk Management
- Cyber Insurance
- Mergers and Acquisitions

## IV. DOES SECURITY RATING REALLY HELPS?

Based on the results evaluated from BitSight Ratings across company size, from microcaps (<$500M) to large caps (15B+). Large caps consistently have lower Ratings, averaging 627 since January 2014. Overall, Ratings tend to move inversely with market cap, indicating higher vulnerabilities as companies grow in size. (Source: IHS Markit)

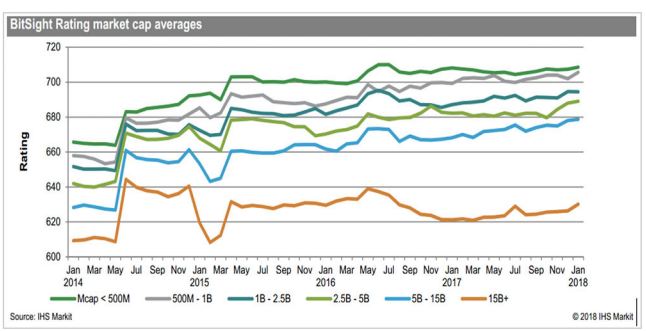


Fig. 4. Bitsight rating vs Company Size (Source: IHS Markit)

Based on the study done for Security Ratings (provided by BitSight) of 27,458 companies. BitSight's data scientists compared this ratings data to a comprehensive set of 2,671 breach events during the same time period. The results demonstrate that 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.

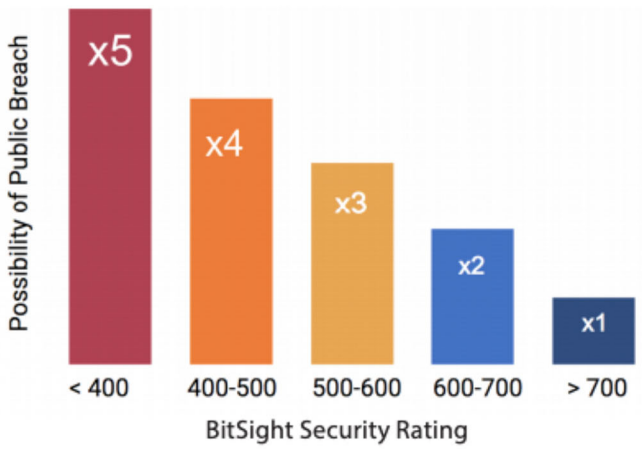


Fig. 5. BitSight Security Rating vs Possibility of Breach (Source: BitSight)

## V. FUTURE ENHANCEMENT

Artificial Intelligence and Machine learning algorithm could be implemented to gather real time breach related, threat or plan of cyber-attacks from the dark or deep web against an organization.

Currently security rating solutions are mainly focused on outside-in threats, however industry demand is very soon going to shift to both outside-in & inside-out approach risk rating. Rating solution also needs to engage combination of both passive and active technique to arrive at a most accurate risk rating for an organization.

## VI. THE CONCLUSION

Organizations today are facing uphill task when managing their risk. Risk ratings help them to understand the impact of the risk and continuous monitoring their cyber health. Organizations can act to mitigate the future attacks based on the existing threat using risk rating. It would help the organization to reduce the risk as well as threats in the effective way.

REFERENCES

[1]https://www.bitsight.com/hubfs/Q218%20How%20BitSight%20Calculates%20Ratings.pdf

[2]https://www.bitsighttech.com/hubfs/Datasheets/BitSight_Security_Ratings_Correlate_to_Breaches.pdf?t=1487883771834

[3]Security Ratings: Enabling A More Secure Global