WHITE PAPER

Making Risk Management More Effective with Security Ratings

April 2014

BITSIGHT

THE STANDARD IN SECURITY RATINGS

EXECUTIVE SUMMARY

With the growth in the number and sophistication of cyber threats and daily reports of security breaches, cyber risk is high on the list of the most significant risks that organizations face. In fact, according to Lloyds Risk Index 2013[1] cyber risk is now the third biggest concern of CEOs and their senior executives, following high taxation and loss of customers. This is not surprising given that during 2013 cyber attacks became more effective and ubiquitous and we continue to see this trend in 2014 with companies disclosing data breaches at a rapid pace.

Although cyber security risk is now top of mind among executives and regulators, measuring and managing security risk levels has been a difficult task. Faced with a constant stream of evolving threats, many businesses spend millions of dollars annually on people, processes, and technologies to protect themselves against cyber risk. However, they have little visibility into the success of these investments.

The situation is more difficult when quantifying the risk of sharing sensitive data with third parties. With functions such as manufacturing, legal, payroll, payment processing and customer service commonly outsourced, companies can have hundreds of business partners they work with at any given point in time. With the outsourcing trend not likely to change any time soon, third party risk management is only going to continue to grow in importance.

This paper discusses some of the security risk management approaches organizations have taken to date as well as a new approach to the growing problem – BitSight Security Ratings. Risk managers today are using BitSight Security Ratings to identify, quantify and mitigate risk throughout their ecosystem. Three specific use cases are discussed in this paper and summarized below.

1. **Organizational Benchmarking:** Organizations are using BitSight Security Ratings to quantify their cyber risk, measure the impact of risk mitigation efforts, and benchmark their performance against industry peers.

2. **Third Party Risk Management:** BitSight Security Ratings help organizations quickly and cost effectively identify the on-going risk of sharing sensitive data with third parties, including business partners, vendors, and acquisition targets.

3. **Increase Awareness, from the Board Down:** BitSight's executive level dash boards are increasingly being used to educate management teams on security issues and provide important data to make risk based business decisions.

[1] Llyods, *Risk Index 2013*, http://www.lloyds.com/news-and-insight/risk-insight/lloyds-risk-index (March 26, 2014)

Today's Approach to Risk Management

As we can see from the regular announcements of data breaches, no one is immune to a cyber attack. Due to the rapidly evolving nature of cyber threats, a strong security posture today could turn into a weak one tomorrow. In fact, BitSight found evidence of compromise on 82% of the companies in the S&P 500 it studied in 2013. Also, even if an organization has a strong security posture, oftentimes it is a third party vendor or business partner that puts an organization at risk.

Most companies today manage security risk as part of their overall IT practice, and 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 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 also spend time and resources ensuring they have all of the appropriate industry certifications and are meeting industry compliance requirements, such as HIPAA, PCI and NIST. Security spending increases globally year after year. However, despite all of these efforts, the frequency of cyber attacks is on the rise. There are few objective metrics to continuously measure a company's security posture and evaluate if it has improved or worsened. Without a quantified baseline, continuous measurement, and comparative data, executives cannot measure the impact of risk mitigation efforts or assess performance against industry peers.

Identifying, assessing and responding to third party security risk is also challenging. Although more and more companies understand the risk of sharing sensitive data with business partners and the need to identify and manage that risk, they often lack the resources to proactively do so. The approach that leading security groups in organizations follow today to measure the IT security stance of partners and vendors is typically to collect data via a requirements checklist or questionnaire, or by asking for an auditor's attestation of compliance with an industry-appropriate standard. Assessment guidance from standards like the Statement on Standards for Attestation Engagements (SSAE) No. 16, ISO 27001, and FedRAMP all come to mind here. Serving as a compendium of best practices, measuring against these standards can give good indicators of where to focus resources and is a good place to start third party evaluation. The challenge is that using these methods alone for assessing security risk is not sufficient, as we know from the growing number of public breaches involving business partners.

> **"Target traces data breach to credentials stolen from vendor"**
>
> *LA Times, January 29, 2014*

A company may be compliant with all the appropriate regulations and have excellent security policies, but may be ineffective in the day-to-day implementation of these policies. Rarely does a security assessment discover how many compromised servers a company is currently running on its network. Also, no matter how complete a checklist or audit is, its results are only a point in time reflection and can not measure the dynamic nature of cyber risk. Even if a penetration test or vulnerability scan is conducted, its results may not be valid the following week. The weakness of current risk management approaches has not gone unnoticed by regulators. In February 2014, National Institute of Standards and Technology issued a Framework for Improving Critical Infrastructure Cybersecurity to help organizations better understand, communicate and manage their cyber risks. This voluntary framework focuses on using business drivers to guide risk management activities and also addresses the need to manage third party risk.

On October 30, 2013, the Office of the Comptroller of Currency (OCC) issued updated guidance on third party risk management. The new guidelines noted eight specific areas of improvement, including continuously monitoring third parties activities and performance. In an article on the OCC guidance[2],Gartner analyst Avivah Litan stated that the guidance was "right on the mark" and that "with more reliance on third parties for all functions, it's important to set these guidelines." Updates to PCI 3.0 and HIPAA regulations have highlighted the increasing pressure to better manage cyber risk in other industries such as healthcare and retail.

[2] Tracy Kitten, "OCC: New Guidance for Third-Party Risks," *Gov InfoSecurity,* October 31, 2013 (http://www.govinfosecurity.com/occ-new-guidance-for-third-party-risks-a-6187)

Complimenting a security assessment with a continuous evaluation of security effectiveness allows organizations to augment their view into the security risks of the extended enterprise and meet these new guidelines and regulations. In addition to gaining visibility into the weaknesses of a network, a data-driven, evidence-based assessment can allow organizations to proactively mitigate new risks as they emerge and identify issues that a regulatory audit was not designed to catch. By taking these steps, organizations can move towards a mature, risk-based security model and away from the more simple checkbox mentality.

Security Ratings: A New Risk Management Approach

For years, credit risk managers have enjoyed the benefit of credit ratings from credit bureaus to make lending, investment and partnership decisions. These ratings are standardized, easy to understand and use, and mostly based on reliable data. Like credit risk managers, security risk managers need data driven, objective and comparable ratings to help them better manage risk. That's where security ratings come in to play.

BitSight Technologies has developed the industry standard for security ratings. BitSight Security Ratings provide an objective, data driven measure of companies' security performance, giving risk managers the ability to measure risk over time.

BitSight Security Ratings are generated on a daily basis and range from 250 to 900 with higher ratings indicating better security performance. To generate the ratings, BitSight gathers and evaluates terabytes of publicly available data on security behaviors from collection points across the globe. Various types of data are used to rate a company, including configuration information and security event data. All of the data used to derive a Security Rating is externally available and collected without any intrusive testing on an organization.

Configuration information represents a measure of how diligent a company is in mitigating risk. Proper configuration and timely patches and updates are good practices to prevent security breaches. Examples of evidence gathered in this category include Sender Policy Framework records, encryption strength, open proxies, and network configuration.

Security events, on the other hand, represent evidence of successful cyber attacks. Given the open and interconnected nature of the Internet, there is a tremendous amount of information that one can learn about security performance. Security events, such as malware distribution, participation in a Distributed Denial of Service attack, and communication with a known botnet command and control server, can tell a story about the kinds of activities that might be happening inside an organization. Although each of these security events does not necessarily equate to data loss, each one is an indication that the organization has been compromised in some manner and should be investigated further.

BitSight gathers this data on a continuous basis, analyzing it for severity, frequency, duration and confidence. Company and industry Security Ratings are updated daily based on the latest data and presented in the BitSight Customer Portal. Alerts are generated upon significant changes in a company's rating. Figure 1 below details this process.

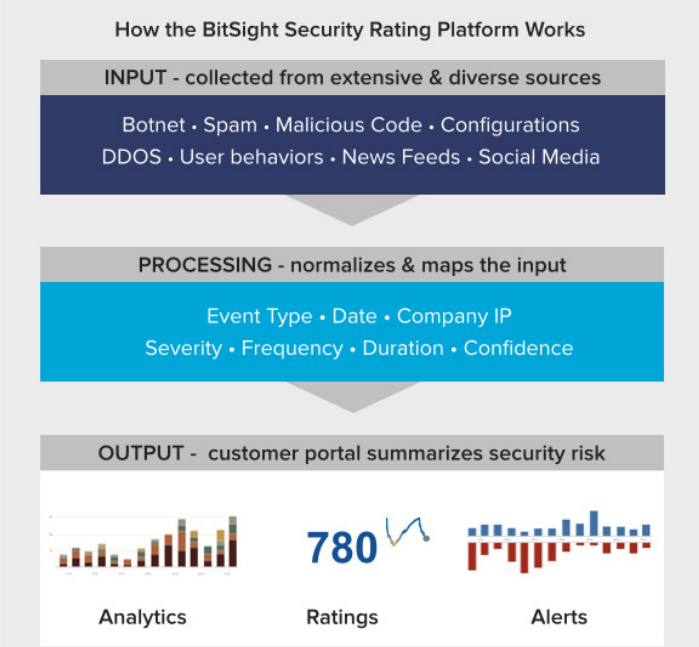

Figure 1: The BitSight Security Rating Platform collects and analyzes data on a continuous basis to generate daily ratings and alerts as needed.

Three Ways Managers Can Use Security Ratings to Mitigate Risk

When it comes to BitSight Security Ratings, there are many ways they can be used as part of an overall risk management practice. Many organizations are still in the dark about the level of security risk they face within their own networks and the risk introduced by business partners. They do not have the resources to measure risk or implement a continuous risk management strategy. Fortunately, BitSight Security Ratings provide cost effective and continuous insight into evolving risk profiles.

Here are three ways organizations have adopted BitSight Security Ratings to proactively manage risk:

1. Benchmark Security Performance

Finance groups measure corporate performance with metrics such as gross margin, earnings per share, and customer retention rates. Operations departments measure performance by metrics such as uptime, latency, and time to resolve customer support issues. But, risk managers lack standard metrics to measure cyber risk. They can certainly look at the number of data breaches and number of compromised machines. But they have no insight into whether the total number of machines compromised globally has also increased. Despite the recent headlines, very few security compromises are publicly disclosed. Many are never even detected.

BitSight Security Ratings for Benchmarking enable organizations to quantify their cyber risk, measure the impact of risk mitigation efforts, and benchmark their performance against industry peers (Figure 2). Some questions that can be answered with Security Ratings include the following:

- Is my security performance increasing or decreasing?
- How does my performance compare to the industry average?
- How do I stack up against my peers?

BitSight provides a detailed view into a company's own security events and configurations. These details can be used to better identify the sources of risk and take swift action to mitigate it. Alerts on significant changes in a company's own rating often provide early warning signs of a bigger problem.

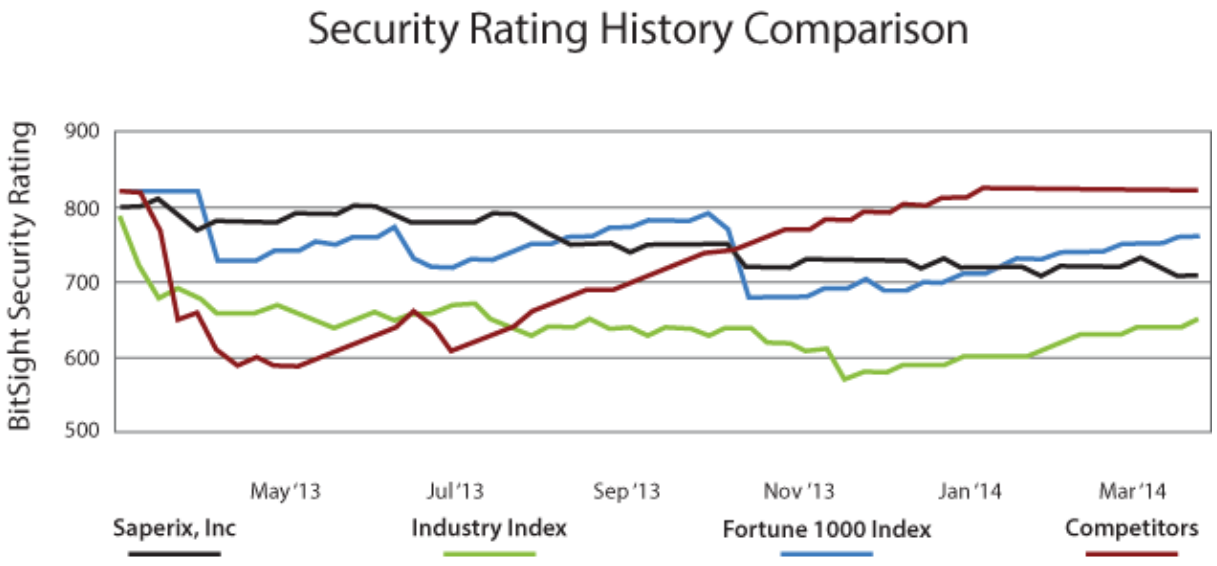

Figure 2: BitSight Security Ratings for Benchmarking allow companies to gain insight into their security performance as it compares over time to peers.

2. Manage Risk Posed by Third Parties

Whether an organization has to manage an abundance of third party vendors, potential new clients, business partners or acquisition targets, continuous measurement is crucial to understanding the risk associated with doing business with them (Figure 3).

BitSight Security Ratings help organizations quickly and cost effectively identify risk before a deal is struck and then continuously monitor that risk throughout the life of the partnership. Organizations use Security Ratings to determine which vendors to assess first, which to assess in more detail, and which partnerships to terminate due to unacceptable risk levels. By helping prioritize, ratings allow organizations to more efficiently manage their resources in order to better identify, quantify and mitigate risk associated with third parties. In addition, BitSight Security Ratings can be used to help meet the growing number of regulations around third party risk management, such as HIPAA, OCC, and PCI-DSS with proactive, continuous monitoring of third party vendors' security effectiveness.

Security risk assessments are also increasingly becoming part of the M&A due diligence process. For acquisition prospects, BitSight Security Ratings help identify the risks and allow the associated mitigation costs to be factored into the overall cost of an acquisition and integration time line.

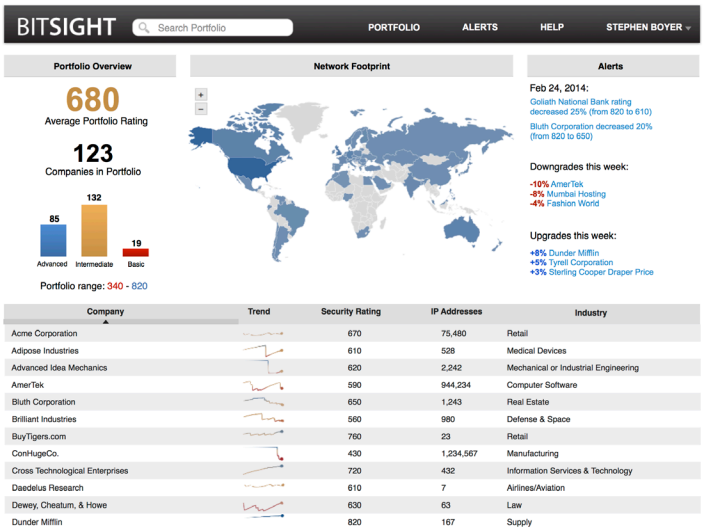

Figure 3: BitSight Security Ratings allow organizations to quickly and easily assess the security performance of third parties.

3. Increase Awareness from the Board Down

With many CEOs and Boards now demanding regular visibility into security risk throughout a company's ecosystem, security practitioners need a way to communicate security risk in business terms. BitSight's executive level dashboards are increasingly being used to educate management teams and provide data to make risk based decisions. Security Ratings provide executives with an easy to understand view of a company's risk level over time and how it compares with others in its industry. They also provide a view of the risk faced by sharing sensitive data with business partners. With Security Ratings, security risk can become an important component of all business decisions.

In addition, detailed reports showing the activity that underlies a Security Rating help to increase awareness among IT security managers. These reports help pinpoint events and configuration issues so practitioners can quickly respond and mitigate the threat.

CONCLUSION

No one is immune from being hacked, and effective continuous risk management is important for companies of all sizes and all industries. In a recent BitSight analysis[3] that focused on the security performance of 460 companies in the Standard & Poor's 500 stock index (S&P 500), BitSight found that collectively, America's largest companies are in weak cyber health. With less than a quarter of companies analyzed utilizing best practices to mitigate the two classes of configuration risk examined (SPF and SSL), it is no surprise that over 80% of them suffered from externally observable security events in 2013. Greater diligence will go a long way in improving cyber health.

The good news is that companies today are making cyber security an executive and board level topic and realize the need for better risk management. With a greater emphasis on cyber security and more proactive diligence with risk management, organizations using BitSight Security Ratings are seeing improvements in their cyber health. Continuous and data driven Security Ratings fill a gap by providing continuous insight into the risks their organizations face and go a long way in managing and mitigating risk in the future.

[3] BitSight Technologies, "Assessing the Cyber Health of the U.S. Economy," February 2014 (http://info.bitsighttech.com/bitsight-cyber-health-sp-500)