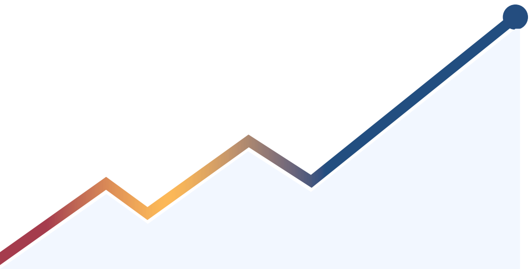
BITSIGHT



Making Risk Management More Effective With Security Ratings

ORGANIZATIONAL BENCHMARKING & BOARD LEVEL REPORTING

THIRD PARTY RISK MANAGEMENT

CYBER INSURANCE UNDERWRITING & ASSESSING AGGREGATE CYBER RISK

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, cybersecurity (specifically cybercrime, data breaches, and IT failures) was identified as the third biggest risk organizations according to a 2016 survey of risk professionals conducted by Allianz[1]. This is not surprising given that the Identify Theft Resource Center recorded 980 major breaches[2] in 2016, with millions of records exposed or compromised.

Although cybersecurity risk is now top of mind among executives and regulators, measuring and managing security risk levels continues to be 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 efficacy 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 and Security professionals at more than 600 organizations today are using BitSight Security Ratings to identify, quantify and mitigate risk throughout their ecosystem. The three specific use cases are discussed in this paper and summarized below.

1. Organizational Benchmarking & Board Level Reporting

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. Many companies are now also using BitSight Security Ratings to report security progress and results to their Board of Directors in language that puts security and risk into business context.

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. Cyber Insurance Underwriting and Assessing Aggregate Cyber Risk

Many of the leading cyber insurers are now using BitSight Security Ratings to get a more accurate, continuous picture of cyber risk posed from applicants as well as policyholders.

[1] Allianz Risk Barometer Top Business Risks 2016

[2] Identity Theft Resource Center 2016 Data Breach Category Summary

TODAY'S APPROACH TO RISK MANAGEMENT

As we can see from the frequency and scale 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 that nearly 80% of organizations across all industries are vulnerable to POODLE or Logjam, both of which are major SSL/TLS vulnerabilities. Even if an organization has a strong security posture, oftentimes it's 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 that they are meeting industry compliance requirements, such as HIPAA, PCI, and NIST, or the European Data Protection Directive. 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.

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 and continuously do so.

Without a quantified baseline, continuous measurement, and comparative data, executives cannot measure the impact of risk mitigation efforts or assess performance against industry peers.

"IT USED TO TAKE WEEKS TO COMPLETE VENDOR ASSESSMENTS. NOW IT TAKES US HOURS. BITSIGHT SECURITY RATINGS FACILITATE SECURITY DISCUSSIONS WITH POTENTIAL VENDORS. IT'S AN INTEGRAL PART OF OUR VENDOR RISK MANAGEMENT PROGRAM."

MICHAEL CHRISTIAN, INFORMATION SECURITY MANAGER OF CYBER RISK & COMPLIANCE, CABELA'S

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. 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 is proven by the growing number of public breaches involving business partners.

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 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.

In its 2016 Semiannual Risk Perspective, the the Office of the Comptroller of Currency (OCC) restated its concern about third and fourth party cyber risk. The regulator, which gave guidance on third party risk management in 2013, identified assessing the effectiveness of banks' third party cyber risk programs as a "supervisory priority". The Securities and Exchange Commission (SEC) has also identified cybersecurity as one of its examination priorities for 2016. SEC examiners have found major gaps in third party risk management efforts of organizations and may make this a focus of future exams. Regulation is not only on the rise in the Financial Services industry. Regulators such as the U.S. Department of Health & Human Services (HHS), Federal Trade Commission, and Federal Energy Regulatory Commission (FERC) have all discussed or pursued enforcement actions for failure to appropriately implement third party risk management programs.

Complementing 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 into play.

BitSight Technologies has developed the industry standard for security ratings. BitSight Security Ratings provide an objective, data driven measure of a company's security performance, giving risk managers the ability to measure risk over time. That's where security ratings come into play.

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 data on compromised systems, security diligence, user behaviors, and data breaches. All of the data used to derive a security rating is externally available and collected without any intrusive testing on an organization.

Compromised systems represents 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. Compromised systems, 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. Many of these threats have been attributed to a higher likelihood of data loss, and each one is an indication that the organization has been compromised in some manner and should be investigated further.

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.

WHAT MAKES A SECURITY RATING?

COMPROMISED SYSTEMS (60%)

+

DILIGENCE (30%)

+

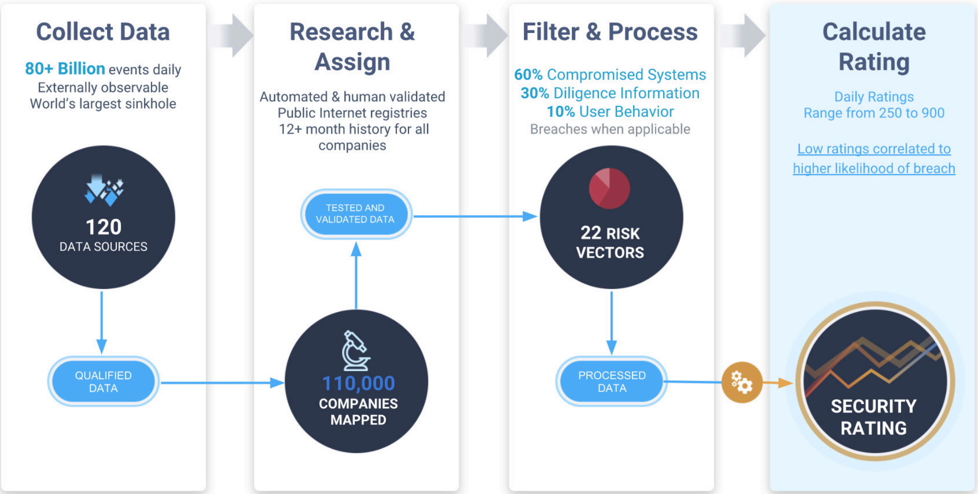
USER BEHAVIOR (10%)

+

DATA BREACHES

=

BITSIGHT® SECURITY RATINGS



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.

User behavior represents any possible risks stemming from employee actions on corporate networks. Examples of risky user behavior include peer-to-peer file sharing, which may introduce malicious software onto networks by downloading a compromised file. Disclosed credentials of employees may also indicate whether employees of a company have had their personal or corporate information compromised as part of a publicly disclosed breach.

Data Breach Events are publicly disclosed incidents of data loss or theft. These include data lost through successful attacks, employee negligence, and hardware theft.

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.

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 principal ways organizations have adopted BitSight Security Ratings to proactively manage risk:

1. Benchmark Security Performance

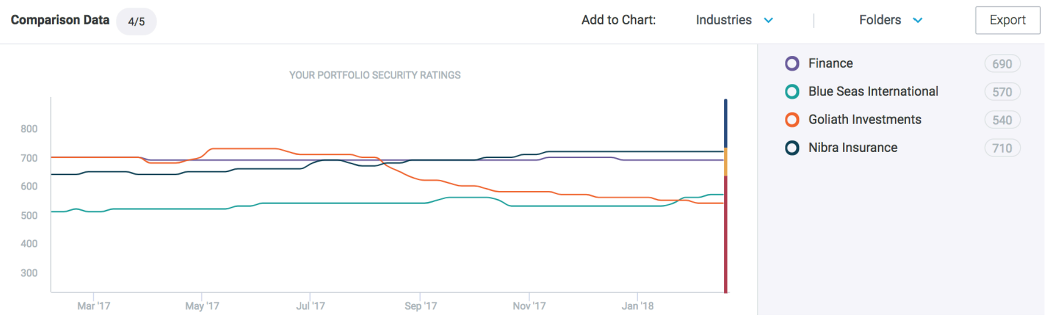
Finance groups measure corporate performance with metrics such as gross margin, earnings per share, and customer retention rates. Operations departments measure performance by metrics such as uptime, latency, and time to resolve customer support issues. But, risk managers lack standard metrics to measure 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 publically 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. Some questions that can be answered with BitSight Security Ratings include the following:

- How has my security performance changed in the last 12 months?
- Is my security performance increasing or decreasing?
- How does my performance compare to the industry average?
- How do I stack up against my peers and competitors?

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.

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.



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

2. Manage Risks Posed By Third Parties

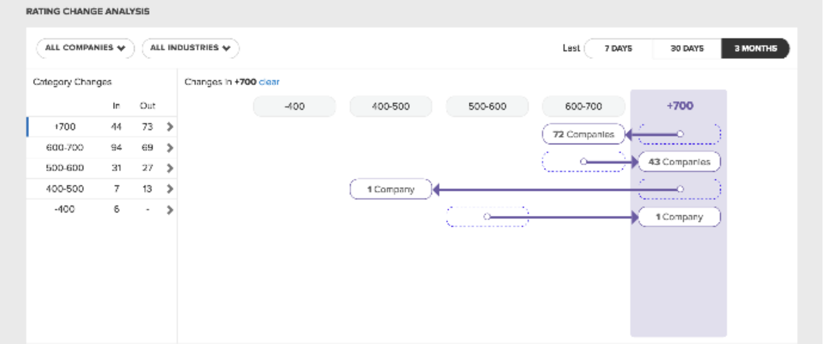
Whether an organization has to manage an abundance of third party vendors, potential new clients, business partners or acquisition targets, continuous measurement is crucial to understanding the risk associated with doing business with them.

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.

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 to 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. Lastly, BitSight's Portfolio Quality Dashboard can give a look into the aggregate risk of your third parties, with a detailed analysis of which companies have improved or declined in a recent timespan.

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.

Organizations can also enable vendor access to the BitSight Security Ratings portal, arming third parties to remediate any lingering issues on their networks themselves. Each company will be given 14 days of complimentary access to the BitSight portal, including forensic information to facilitate the remediation of any cyber threats occurring on networks.



RATING CHANGE ANALYSIS

Category Changes

	In	Out
+700	44	73
600-700	94	69
500-600	31	27
400-500	7	13
-400	6	-

Changes in +700 clear

Rating Change Analysis allows you to identify how the ratings of companies have changed in the last week, month, or three months. Customers can pinpoint groups of companies that have had significant rating drops that span more than one rating category.

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.

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 experiencing a data breach, but effective continuous monitoring of cybersecurity risks is an important step for companies of all sizes and all industries to mitigate risk. The good news is that companies today are making cybersecurity an executive and board level topic and realize the need for better risk management. With a greater emphasis on cybersecurity 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.

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.

"We are able to benchmark our security against that of our competitors. We can share that information with our senior leadership and board of directors, and give them a sense of comfort that our program is on track."

ABOUT BITSIGHT TECHNOLOGIES

BitSight transforms how companies manage information security risk with objective, verifiable and actionable Security Ratings. Founded in 2011, the company built its Security Ratings Platform to continuously analyze vast amounts of external data on security issues. Seven of the largest 10 cyber insurers, 80 Fortune 500 companies, and 3 of the top 5 investment banks rely on BitSight to manage cyber risks.

FOR MORE INFORMATION

BitSight Technologies
125 CambridgePark Drive
Suite 204
Cambridge, MA 02140

www.bitsighttech.com
sales@bitsighttech.com