ESG Brief

Utilizing Security Ratings for Enterprise IT Risk Mitigation

Date: June 2014 **Author:** Jon Oltsik, Senior Principal Analyst

Abstract: *What do large enterprises need in order to address increasingly dangerous cyber threats? Actionable, objective, and continuous intelligence into security risk across their ecosystems. They need objective metrics to measure risk and benchmark performance as well as detailed information to mitigate known threats. Furthermore, this intelligence must help them recognize risks to internal networks, their partners' networks, and their industries. BitSight Technologies provides security ratings that measure company and industry security performance and can help CISOs and Chief Risk Officers mitigate risk, streamline security operations, and engage business executives in their cybersecurity strategies.*

Overview

A few years ago, IT security was a niche activity within IT departments. More recently, however, cybersecurity has become part of boardroom business discussions and political debates about national security. This transition occurred for many reasons but one simple explanation is that recent cyber-attacks are more frequent, sophisticated, and damaging than they were in the past. This change is evidenced by recent ESG research indicating that 30% of security professional believed the overall malware landscape was much worse in 2013 than it had been two years previously, while another 37% said the overall malware landscape had grown somewhat worse.[1] Aside from opinions alone, ESG research also revealed that nearly half (49%) of enterprise organizations reported suffering a *successful* malware attack in the previous 24 months (a "successful malware attack" is defined as a malware attack that compromises an IT asset resulting in some type of negative ramification such as data theft, system downtime, the need to reimage a system, etc.).[2] Alarmingly, 22% of organizations have experienced more than 26 successful malware attacks in the past two years.[3]

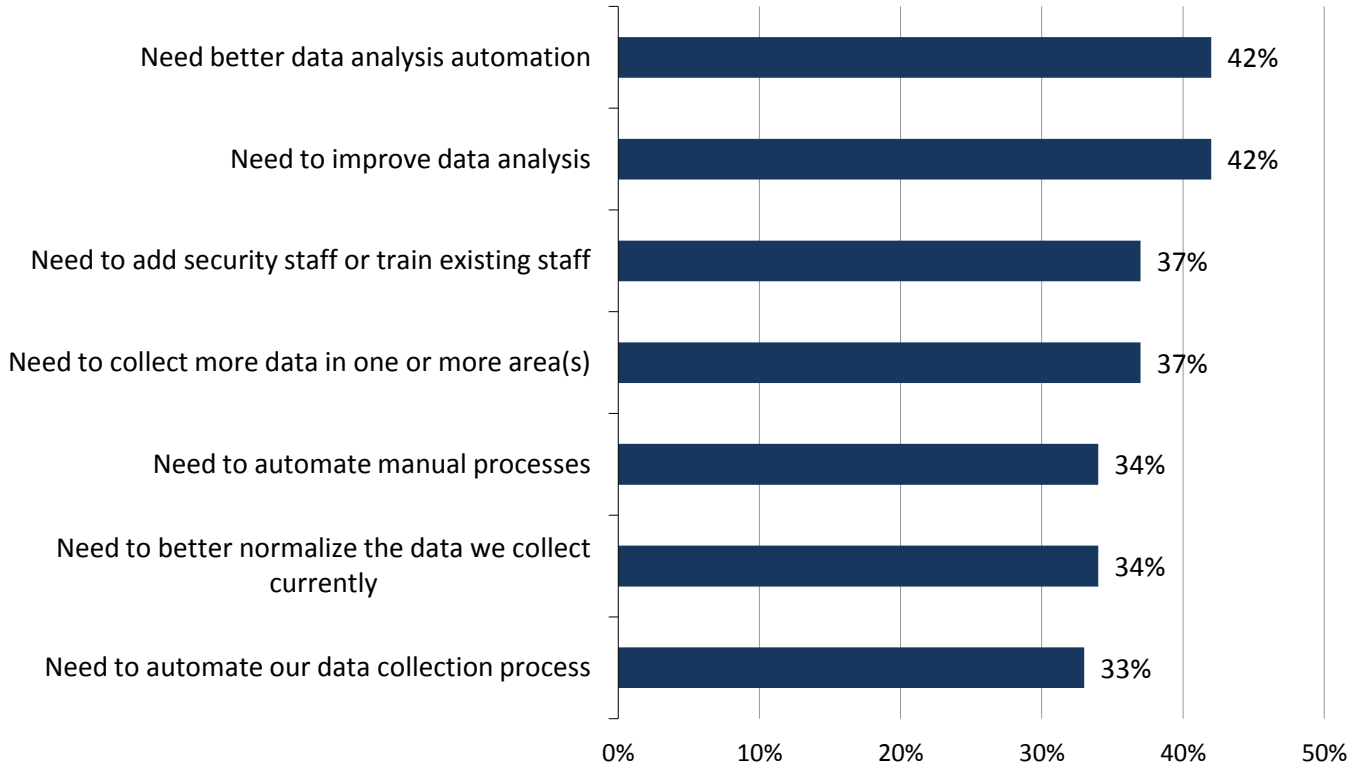
Large Organizations Need Better Intelligence for Risk Management

With the rise of sophisticated targeted cyber-attacks, many enterprises are investing in new types of security technologies for incident prevention, detection, and response. While it is certainly worthwhile to add layers of security, there is also an acute need for more fundamental improvements. According to ESG research, only 13% of enterprise organizations claim that they have a complete IT risk profile (i.e., percentage of vulnerable systems, remediation activities, controls violations, etc.).[4] This means that many organizations are "flying blind" through current threats and vulnerabilities. When asked what they would need to bridge this gap, security professionals pointed to the need to improve and automate data analysis, add/train existing staff, and collect more data in one or several areas (see Figure 1).[5]

[1] Source: ESG Research Report, *Advanced Malware Detection and Protection Trends*, September 2013.
[2] Source: Ibid.
[3] Source: Ibid.
[4] Source: ESG Research Report, *The Emerging Intersection Between Big Data and Security Analytics*, November 2012.
[5] Source: Ibid.

Figure 1. Steps Organizations Would Need to Take to Make IT Risk Profile Reports 100% Complete

Which of the following steps would your organization need to take in order to achieve the goal of IT risk profile reports that are 100% complete? (Percent of respondents, N=224, multiple responses accepted)



Source: Enterprise Strategy Group, 2014.

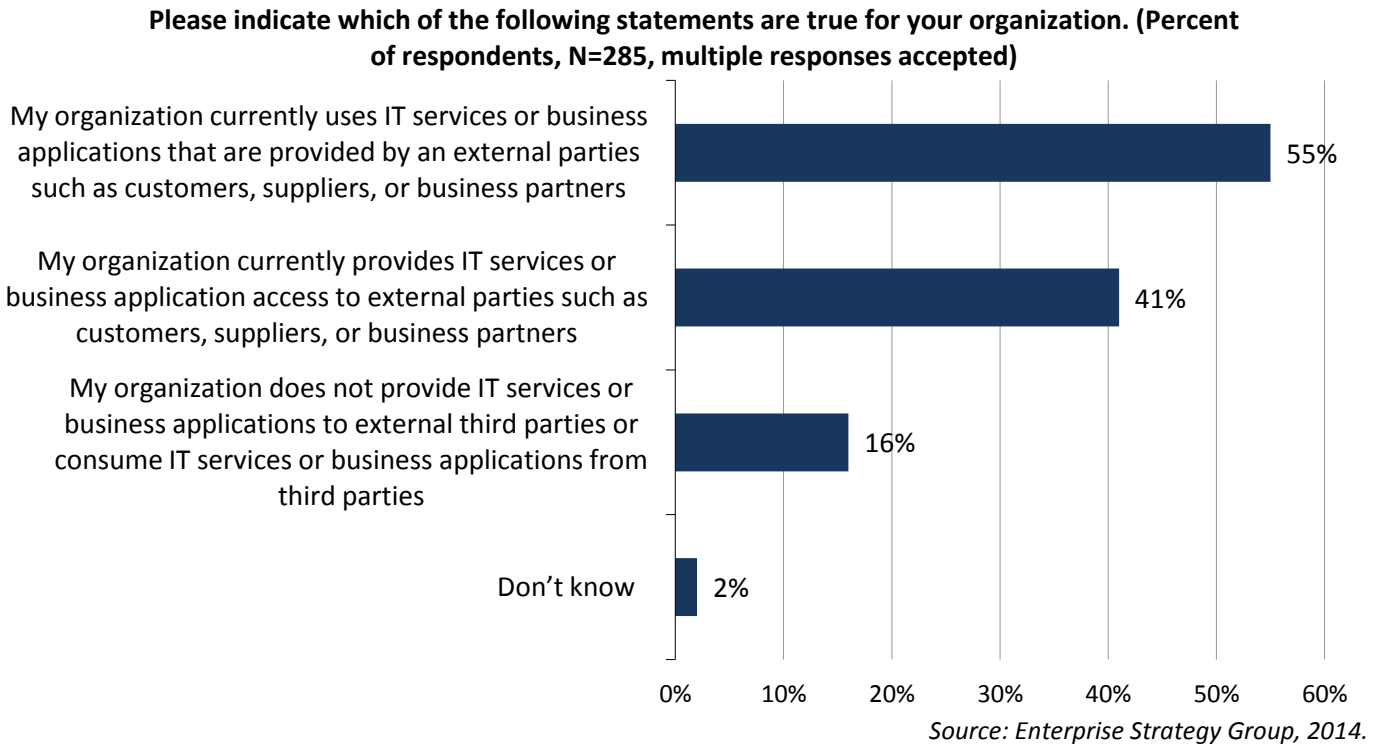
Cyber Risk Management Circa 2014

The ESG research presents an alarming situation: Many organizations don't have a clear picture of what systems, devices, and users are on their networks at any time and do not have a way to efficiently identify, measure, and continuously monitor their risk profiles. This situation should be of grave concern to CISOs because current IT risk management best practices demand:

- **Continuous risk measurement and monitoring.** IT security managers need timely data about the behavior on their networks and the configuration status of these systems. They need an objective way to measure the performance of their security investments and policies and compare their performance to peers. In addition, CISOs need an outside-in perspective of network activities to assess whether internal networks are hosting botnets, distributing SPAM or adware/spyware, or communicating with known command and control servers.
- **Actionable intelligence.** Veteran IT professionals are familiar with the acronym GIGO (garbage in, garbage out). Clearly, CISOs need additional data to assess risk, but security intelligence must also be granular, detailed, and actionable. In other words, security professionals need the right data so they can understand and quickly react to threats, vulnerabilities, and behaviors associated with specific IT applications, data, services, and systems.
- **Risk management metrics.** Since cybersecurity has become a boardroom issue, CISOs need the right set of metrics to communicate IT risks associated with the organization, the cyber supply chain, and the overall industry. These metrics can be used to help security managers quantify and compare risks so that business managers have appropriate guidelines for decision making.

- **A purview across the cyber supply chain.** In the past, most organizations focused risk management activities on internal systems, networks, and applications. This type of self-assessment is critically important but it is no longer adequate alone. Why? Enterprise IT applications and infrastructure are often inexorably linked to a mix of business partners, customers, and suppliers. In fact, previous ESG research indicates that 55% of enterprises consume IT services from other organizations, while 41% provide IT services to an assortment of third parties (see Figure 2).[6] To paraphrase an old cybersecurity adage, the cyber supply chain is only as strong as its weakest link. The recent cyber attacks on Target, Yahoo, and T-Mobile were due to breaches in partner networks. To manage this risk, CISOs need to understand the risk of sharing sensitive data with business partners, such as HR and payroll service providers, payment processors, and customer service providers.

Figure 2. Enterprise IT Extends Beyond the Internal Network



Source: Enterprise Strategy Group, 2014.

Introducing BitSight Technologies

Improving internal and cyber supply chain risk management won't be easy, especially if CISOs are forced to work with numerous third-party tools and services to collect, aggregate, and analyze disparate security intelligence feeds. Regrettably, this is often the case, forcing organizations into manual data analysis or building customized tools for data ingestion, normalization, and processing.

One alternative to this security intelligence morass comes from BitSight Technologies of Cambridge, MA, which rates companies' security performance. BitSight's cloud-based intelligence platform collects terabytes of data each day on security incidents and configurations from sensors distributed across the global Internet. Through its analysis, BitSight discovers and identifies cyber risks such as botnets, SPAM, malware, DDoS traffic, poor e-mail server configurations, and weak or expired SSL certificates. BitSight analyzes the severity, frequency, and duration of these cyber events and maps them to individual organizations' known networks. Then, using a sophisticated algorithm, BitSight generates ratings daily on companies and industries.

[6] Source: ESG Research Report, *Assessing Cyber Supply Chain Security Vulnerabilities Within the U.S. Critical Infrastructure*, November 2010.

Through its platform and service offerings, BitSight provides actionable Security Ratings that can help enterprise organizations manage and mitigate IT risk. In fact, CISOs can leverage BitSight Security Ratings across a multi-phased risk management improvement initiative (see Table 1).

Table 1. BitSight Security Ratings

Activity	Requirement	Benefit
Improve internal risk management	Continuously monitor and measure risk levels and security performance. Get the details required to quickly remediate existing compromises and vulnerabilities.	Quickly and cost-effectively prioritize and remediate issues. Understand whether your risk is increasing or decreasing, whether your security investments are making a difference, etc.
Benchmark performance with objective metrics	Measure external risk of organization in comparison to key industry leaders and competitors. Arm business leaders with these metrics so they can understand and incorporate risk into business decisions.	Use industry ratings as metrics to communicate risk levels and performance with management and the board. Make security risk a part of business decisions. Include objective third-party data as a supplement to internal analysis and metrics.
Manage supply chain risk	Gather intelligence on business partners, customers, and suppliers that have access to the organization's network, applications, and sensitive data. Create an objective system to evaluate risk when onboarding a new partner and continuously manage that risk.	Lower the risk of breach via a third party.

Source: Enterprise Strategy Group, 2014.

- **Internal risk management improvement.** Many CISOs recognize that they need to "get their house in order" by embracing continuous monitoring and advanced security analytics. The goal? Identify, measure, and mitigate risk in a timely manner and measure performance over time. BitSight Security Ratings can be used by companies to assess the impact of their security policies and investments over time and compare it with their industry, peers, and competitors. CISOs can also use BitSight's data to help them prioritize remediation activities and adjust security controls. BitSight provides configuration information on externally facing machines and detailed information on malicious activities (i.e., malware proliferation, DDoS traffic, SPAM distribution, etc.) emanating from an organization's network as well as the frequency, duration, and severity of these activities. BitSight also digs into these events by providing specific information about the origin of the traffic, source/destination IP addresses, the server name, and a risk score associated with each type of incident. This intelligence can help organizations mitigate risks as they arise.
- **Benchmark and compare performance with objective metrics.** CEOs and boards of directors read about data breaches each day in the Wall Street Journal but are often frustrated by the lack of tangible data available to measure risk. BitSight industry benchmarking can help here with Security Ratings associated with industries and individual firms. These benchmarks can also be supplemented with detailed BitSight intelligence about the organization itself, which can provide senior business executives with an overview of how they compare with peer organizations and how their industry compares with others. The BitSight data is especially useful for intelligence sharing when cyber criminals target particular industry segments.

- **Cyber supply chain risk management discovery and assessment.** Once internal risk management programs are underway, CISOs should move quickly to address IT risks associated with the plethora of third-party IT connections coming from external users and machine-to-machine integration. In this case, CISOs can use BitSight to monitor and analyze the network activities of key business partners, looking at the frequency and severity of malicious activities. This intelligence can certainly help improve current cyber supply chain risk that is often based upon point-in-time security audit checklists performed on an annual basis. Smart CISOs will use the BitSight intelligence as a catalyst to institute risk management communications, processes, and requirements across the extended IT partner ecosystem.

By leveraging BitSight through this type of phased approach, enterprise organizations can accomplish several goals. First, they can improve risk management processes as they relate to internal IT and the supply chain. Second, BitSight can help streamline incident response by automating today's manual security analysis and investigation activities. Finally, BitSight can help CISOs work with business executives by providing objective data and metrics for cybersecurity decision making.

The Bigger Truth

Sun Tzu, the author of *The Art of War*, once stated: "If you know your enemy and know yourself, you need not fear the results of 100 battles." Unfortunately, many organizations have numerous limitations in both areas because they don't have the right intelligence about internal or enemy activities. This is a fundamental problem that can't be fixed by implementing new types of anti-malware technologies at the network perimeter.

So what's needed? Knowledge. In this case, CISOs need the increased visibility into their IT networks, their partners' networks, their cyber adversaries, and their peers. Armed with this knowledge, they can implement the right tactics and strategies to support business goals while mitigating risk. This is exactly what CISOs are paid to do.