**Input to the Commission on Enhancing National Cybersecurity:**

**The Impact of Security Ratings on National Cybersecurity**

Submitted on September 9, 2016 by
Jacob Olcott
Vice President, BitSight Technologies

## (1) Executive Summary

The President charged the Commission on Enhancing National Cybersecurity with making policy recommendations to enhance national cybersecurity for the future. To do so, the Commission must evaluate the current state of national cybersecurity. But how?

How can the Commission quantitatively measure the cybersecurity performance of thousands of large, medium, and small organizations across dozens of economic sectors, as well as the government itself? Given the Commission's short lifespan and limited number of participants, not to mention the dynamic, ever-changing nature of cybersecurity, how can the Commission obtain a vast amount of actionable, understandable metrics that measure both historical and real-time organizational performance?

This is not a challenge unique to the Commission. In fact, organizations ranging from financial institutions to insurance underwriters to electric utilities to major retailers all seek answers to similar questions. For these companies, meaningfully assessing the cybersecurity of their business associates in real-time, at scale, and cost-effectively is critical to managing cyber risks from third party vendors/suppliers, underwriting cyber insurance policies, benchmarking organizational performance against peers/competitors, conducting better due diligence during the merger/acquisition process, and assessing aggregate risk.

So how do they do it?

The world's most sophisticated and respected organizations use Security Ratings. Much like credit ratings, Security Ratings are generated through the analysis of externally observable data across a variety of risk categories mapped to an organization's known networks. Security Ratings continuously measure security performance. This data-driven, outside-in approach requires no information from the rated entity, allowing for ratings to scale without conflicts of interest.

Security Ratings have become an important foundation for many business relationships, but there are also many national policy implications for Security Ratings. Security Ratings can help policymakers understand the current state of national cybersecurity, measure cybersecurity performance among different sectors, assess the impact and effect of previous national policies on sector-wide performance, and make data-driven decisions about future cybersecurity policy.

As the pioneer of the Security Ratings market, BitSight Technologies believes it is important for the Commission to understand the role that an emerging technology like Security Ratings plays in addressing some of the most critical issues in cybersecurity today. This paper provides background information about Security Ratings, as well as some data about the current state of cybersecurity that may be useful to the Commission. BitSight is pleased to provide any additional data and research for the Commission and its members at your request.

**(2) About BitSight**

BitSight is transforming how companies manage information security risk with objective, verifiable, and actionable Security Ratings. BitSight's Security Rating Platform continuously analyzes vast amounts of external data on security issues and behaviors in order to help organizations manage third party risk, underwrite cyber insurance policies, benchmark performance, conduct M&A due diligence, and assess aggregate risk. BitSight was founded in 2011 and is based in Cambridge, MA.

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 continuously 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. BitSight's sophisticated algorithms analyze the data for severity, frequency, duration, and confidence to create an overall rating of that organization's current security health. All of the data used to derive a BitSight Security Rating is externally available and collected without any intrusive testing on an organization.

Over 450 companies across all key verticals trust BitSight Security Ratings, including 60 of the Fortune 500, top investment banks and private equity firms, several of the Big 4 accounting firms, and many of the world's leading cyber insurance carriers. BitSight is backed the National Science Foundation, and has also funding from prestigious venture capital firms and leading telecommunications organizations across the world, including Comcast, Liberty Global, and Singtel. BitSight was recognized as a Gartner "Cool Vendor" in 2015.

Jacob Olcott, vice president at BitSight Technologies, is providing this input to the Commission on behalf of BitSight. He has spent over a decade shaping national U.S. policy around cybersecurity. He served as legal advisor to the Senate Commerce Committee, where he acted as then-Chairman John D. Rockefeller's lead negotiator on comprehensive cybersecurity legislation and led an investigation into corporate cybersecurity disclosure practices that resulted in SEC guidance on the subject in 2011. He also served as counsel to the House of Representatives Homeland Security Committee where he led investigations and hearings into cybersecurity practices within critical infrastructure and U.S. government departments and agencies. He previously managed the cybersecurity consulting practice at Good Harbor Security Risk Management. He completed his education at The University of Texas at Austin and the University of Virginia School of Law. He currently teaches a class on cybersecurity policy at Georgetown University's School of Foreign Service

## (3) Why Security Ratings?

There are two very important global trends that help explain the emergence and widespread use of Security Ratings: (1) growing recognition and awareness by organizations of **third party cyber risk - also known as "vendor risk" or "supply chain risk"** and (2) growing concerns among senior executives and officers about **legal liability for organizational cybersecurity failures**.

### a) Third Party Cyber Risk is Now Ubiquitous; Managing It Requires Data-Driven, Real-Time Solutions.

As organizations have increasingly outsourced technology infrastructure and other business processes, the number of business to business relationships have skyrocketed. Companies can have dozens, hundreds, or even thousands of third party business relationships. Many of these third party organizations (vendors, contractors, business associates, service providers, etc.) have access to sensitive data or, in other cases, direct network access into the first party organization. As a result, measuring and evaluating cybersecurity risk associated with third parties has become a critical business issue. It has become quite common for organizations to spend a significant amount of time building processes around "third party risk management," "vendor risk management," or "supply chain risk management."

Cyber attacks against third party organizations have risen dramatically. In fact, some of the most well-known data breaches in recent years occurred as a result of a weakness exploited in a third party. For instance, in the 2013 Target data breach, attackers gained access to Target's networks through Fazio Mechanical Services, a contracted HVAC provider which was provided direct network access to Target's computer networks. This business had unrestricted access to all of Target's networks, and attackers were able to steal over 40 million credit card numbers, creating headlines and panic for businesses and consumers.

Not all third party cyber risk is posed by third party organizations with "direct" connectivity to the first party. In the case of the 2015 Office of Personnel (OPM) data breach, third parties were also involved. Intrusion of OPM's networks occurred after stolen credentials from KeyPoint Government Solutions (a contracted background check provider) provided attackers with access to OPM databases. KeyPoint did not have a direct network connection to OPM. Moreover, OPM stored a sizeable amount of its data on Department of the Interior (DOI) servers, which had also been compromised months prior. For OPM, both KeyPoint and the DOI were critical third parties that were compromised and allowed easier access to OPM's data.

Cyber attacks against third parties have become commonplace for three main reasons. First, organizations rely on more third parties for key business functions that used to be performed in-house. With payroll, HR, legal, sales, PR, and even product development functions being outsourced, more third parties have access to more sensitive business information, which presents a great challenge to protect that data. Second, business environments have become

more interconnected, which means that more third parties have been granted direct access to the corporate network to perform essential job functions. This privileged access is great to achieve business objectives, but it also creates greater risk. Third, as first party organizations improve their cyber defenses, attackers are increasingly searching for the weakest links. Smaller businesses often have fewer resources to protect their environments and represent easier attack vectors for the bad guys. Given their access to sensitive data or even the broader network itself, third parties represent great targets.

So how do organizations address these risks? How can an organization assess the security of a third party? Can an organization trust its third parties to report incidents in a timely fashion? How can organizations verify that its third parties meet their security requirements and expectations?

For years, leading security groups collected qualitative security information from their third party vendors through various "point in time" methods: issuing a requirements checklist or questionnaire, asking for an auditor's attestation of compliance with an industry-appropriate standard (e.g. Statement on Standards for Attestation Engagements No. 16, ISO 27001, NIST SP 800-53), or requesting documentation related to a penetration test. On some occasions, organizations ask to perform their own annual on-site inspections or penetration tests on a third party.

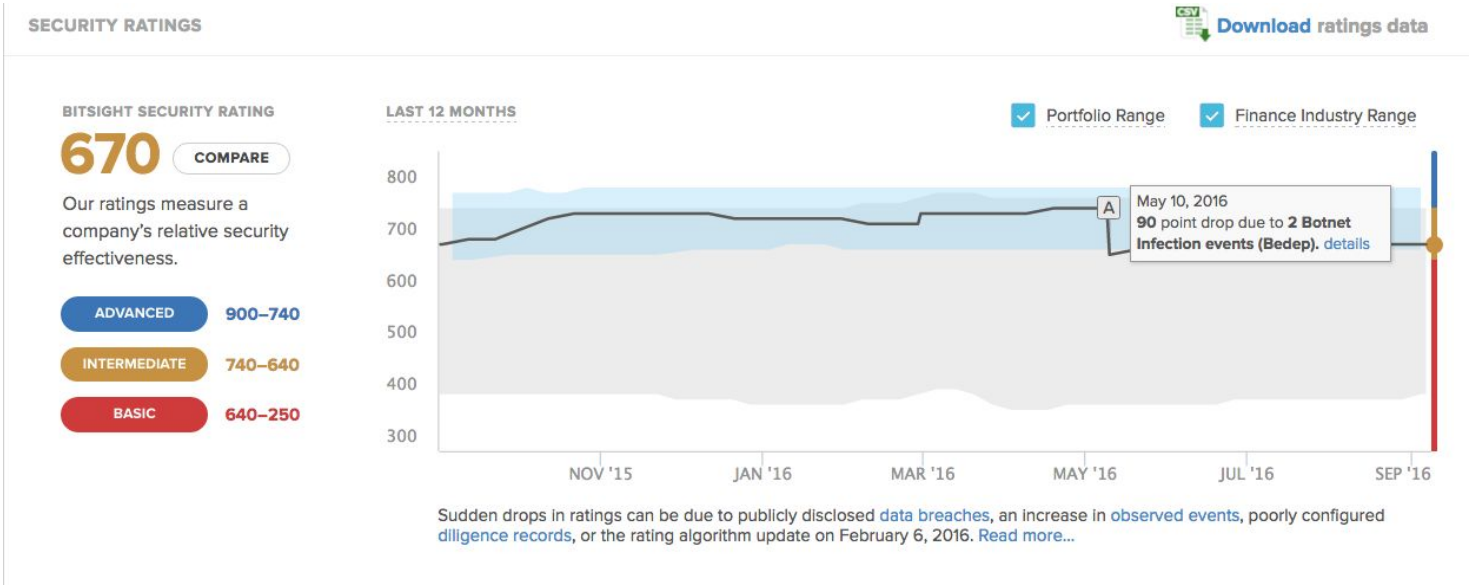
Security groups have discovered that using these methods alone for assessing security risk of third party is not sufficient: a company may be compliant with all the appropriate regulations and have excellent security policies, but may be ineffective in the day-to-day implementation of these policies. Regardless of 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.

This realization has led organizations to use tools that **continuously monitor the cybersecurity of their third parties**, including Security Ratings. These tools allow organizations to quantify cyber risk and measure the impact of risk mitigation efforts. Ultimately, they can also help organizations identify which third parties to consider working with, or which to terminate.

Organizations with third party connections are not the only ones concerned. It is important to understand that there are **many types of organizations concerned about the cybersecurity posture of a third party** that are turning towards quantitative, objective data to make business decisions. For instance, over the last decade, insurance carriers have started to underwrite cybersecurity insurance policies. As these policies have become more popular, insurance carriers are challenged to sufficiently measure the security posture of a growing pool of applicants. Historically, insurers could only rely on questionnaires, penetration tests and on-site assessments, methods that can be effective but also time consuming, expensive and only provide a point in time snapshot of performance. In order to streamline the underwriting

application process, insurers are now incorporating data-driven tools - including Security Ratings - that provide insight into past and current cyber security performance of applicants.

Furthermore, businesses actively looking to acquire companies are moving beyond the traditional qualitative assessment processes and are incorporating quantitative security data - including Security Ratings - into their diligence analysis prior to making a deal. Unlike well documented financial reporting, businesses have trouble gaining visibility into the cybersecurity performance of an acquisition target. As companies look to innovate and strengthen their organizations through mergers and acquisitions, they are using automated tools like Security Ratings that enable them to continuously measure security performance throughout the deal lifecycle.




*BitSight Security Ratings Range on a scale of 250-900.*

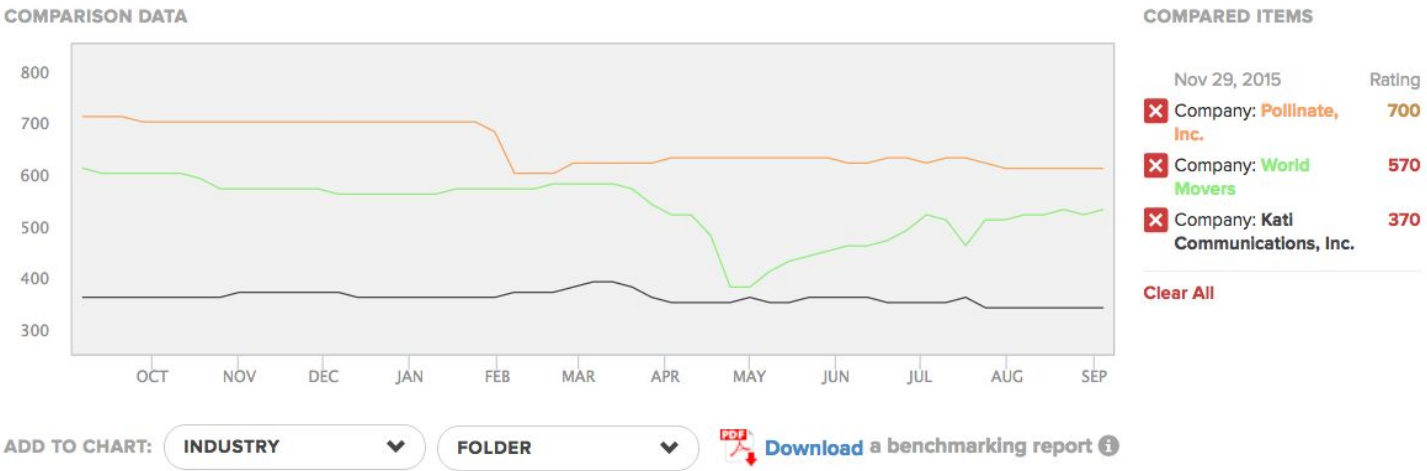
For many businesses today, managing these third party risks with Security Ratings is not a hypothetical matter. Security Ratings are a well-understood concept with a defined market segment with growing demand. Gartner, a leading IT research and advisory firm recently included Security Rating Services (SRS) in its first Hype Cycle for Risk Management. Gartner and other advisory firms are now encouraging organizations to adopt Security Ratings as part of a continuous monitoring program for third party cyber risk management. Moreover, organizations are now openly talking about the efficacy and value that security rating services bring to mitigating third party risk.

**b) Senior Executives and Corporate Directors Face Growing and Uncertain Legal Liability for Organizational Cybersecurity Failures and Must Consume Cybersecurity Performance Metrics.**

The second global trend to understand is that corporate directors and executives face legal liability for their organization's cybersecurity failures, which is leading them to spend much more time consuming metrics about the state of their organization's cybersecurity programs and how that program compares with other peers/competitors. Liability is not only an issue for companies in regulated sectors. For instance, while many are familiar with the material financial loss that Target suffered during its 2013 data breach, fewer realize that Target's CEO and CIO were fired, several key board members were nearly removed by shareholders, and the company's executives and directors were encumbered by nearly 100 separate lawsuits alleging breaches of fiduciary duty and failure to appropriately manage risk to the company.

Companies of all shapes and sizes - public or private, for profit or nonprofit, etc. - are now focusing on cybersecurity as an important point of discussion at Board meetings. With so many data breaches made public, corporate directors are increasingly interested in avoiding actions that expose the organization to regulatory fines, lawsuits, or reputation damage.

To reduce the risk of a cyber breach and the legal liability that would accompany that incident, executives and officers are becoming more directly involved in overseeing their organization's cybersecurity programs, including requesting more information from information technology teams about the organization's cybersecurity performance, including metrics, key indicators, and benchmarking against peers and the industry as a whole.




*Security Ratings allow users to compare the ratings of businesses by their industry, or the types of vulnerabilities or infections present on their networks. (All companies fictitious.)*

The result of increased attention by executives and officers is that CISOs and CIOs must provide additional metrics and performance measurements to help satisfy concerns about the effectiveness of their cybersecurity programs. Frequency of Board-level cybersecurity reporting has increased dramatically, as has the substance of the discussions. Directors are seeking

more details on their company's cybersecurity strategies on a more frequent basis. Beyond the sheer number of briefings, CISOs are now also challenged to translate their initiatives into business terms so that directors can best understand how the cyber program has been constructed and whether there are any critical gaps.

What are the key cybersecurity metrics that organizations discuss internally? How are these communicated to the board? How do CISOs and CIOs obtain these measurements in a real-time basis?

While organizations use a variety of internal data and metrics to evaluate cybersecurity performance, standardized Security Ratings have become an important way to quickly identify and measure key performance metrics internally, including metrics around "detection deficit." For many companies, the time that lapses between a breach and its discovery remains far too long. Many companies do not possess the ability to detect a cyber incident until long after the incident occurred. Reducing this detection deficit can dramatically lower the severity and cost of a cyber incident. Boards must understand the process by which their companies detect incidents and use the "detection deficit" as a key accountability metric.

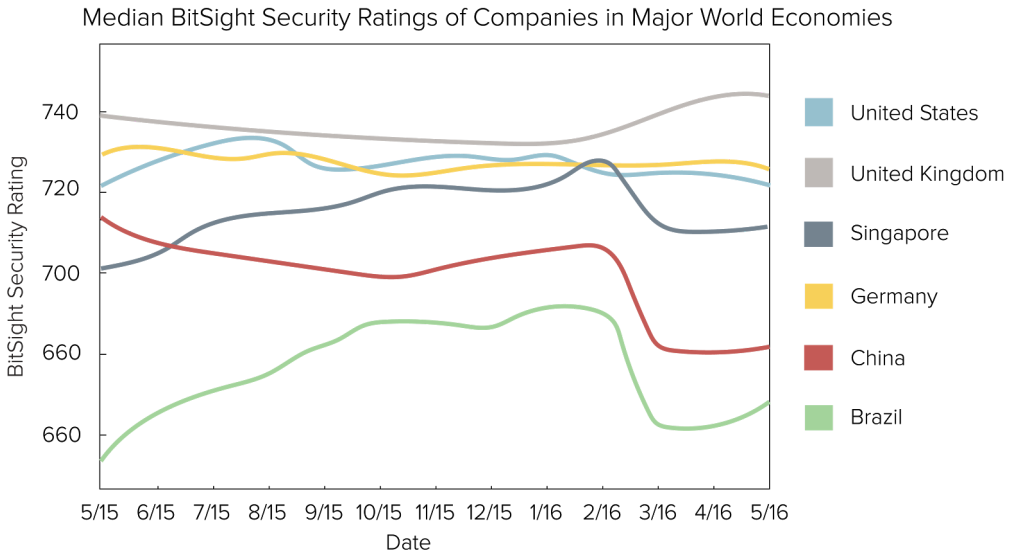
In addition to internal cybersecurity performance metrics, cybersecurity benchmarking data (e.g. peer and industry-wide comparison) is also being reported to senior executives and boards. Most companies use benchmarking processes to measure performance in key business functions such as customer service, human resources and corporate strategy. The same is now true in cybersecurity. Tools like Security Ratings provide a quantified and comparative view of cybersecurity performance over time, allowing users to effectively communicate to the board. By showing the board cybersecurity performance in relation to peers and actionable high level network performance metrics, Security Ratings users have been able to demonstrate program improvements, spotlight weaknesses or areas for improvement, and advocate for increased cybersecurity resources.

## (3) Data for Policymakers

While hundreds of commercial companies consume Security Ratings for various reasons, policymakers also have an interest in the data collected through Security Ratings. BitSight collects a wide variety of data about cybersecurity performance across various sectors. The charts and data below provide just a small sample of the data sets that can help policymakers understand the current state of national cybersecurity, measure cybersecurity performance among different sectors, assess the impact and effect of previous national policies on sector-wide performance, and make data-driven decisions about future cybersecurity policy.

### a) Organizational Performance in Different Countries

BitSight recently looked at the security performance of organizations across major world economies, including: the United States, United Kingdom, Singapore, Germany, China, and Brazil. Researchers found that companies with more than 50% of their networks located in the United Kingdom, United States, and Germany tend to be more secure than other nations.



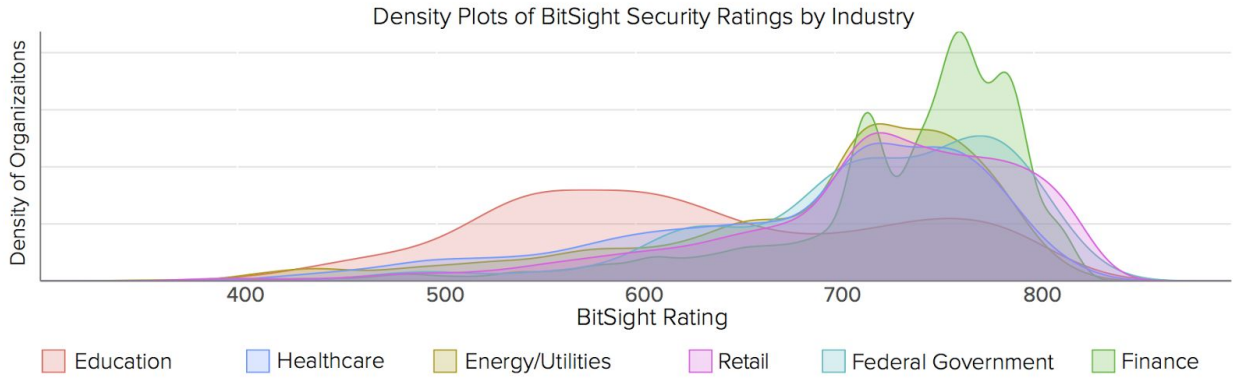

*Source: BitSight Insights - Analyzing Security Performance Metrics Across Major World Economies (2016)*

While companies in the United States tended to perform well, they had the second highest rate of machine compromise on corporate networks. Specifically, US companies had a high rate of botnet infections. These infections are direct evidence that an outside attacker has gained access and/or control of a system. In fact, BitSight researchers found that companies with pervasive rates of compromised machines on their networks are more than two times likely to experience a data breach.

### b) Organizational Performance by Sector

BitSight frequently reports on industry-specific trends. We typically find that financial organizations tend to have the best security posture relative to companies in other industries. Other industries such as Education and the Energy/Utilities sector often struggle to mitigate cyber risk for a variety of reasons. The chart below contains the ratings densities of thousands of companies across 6 key sectors of the economy.

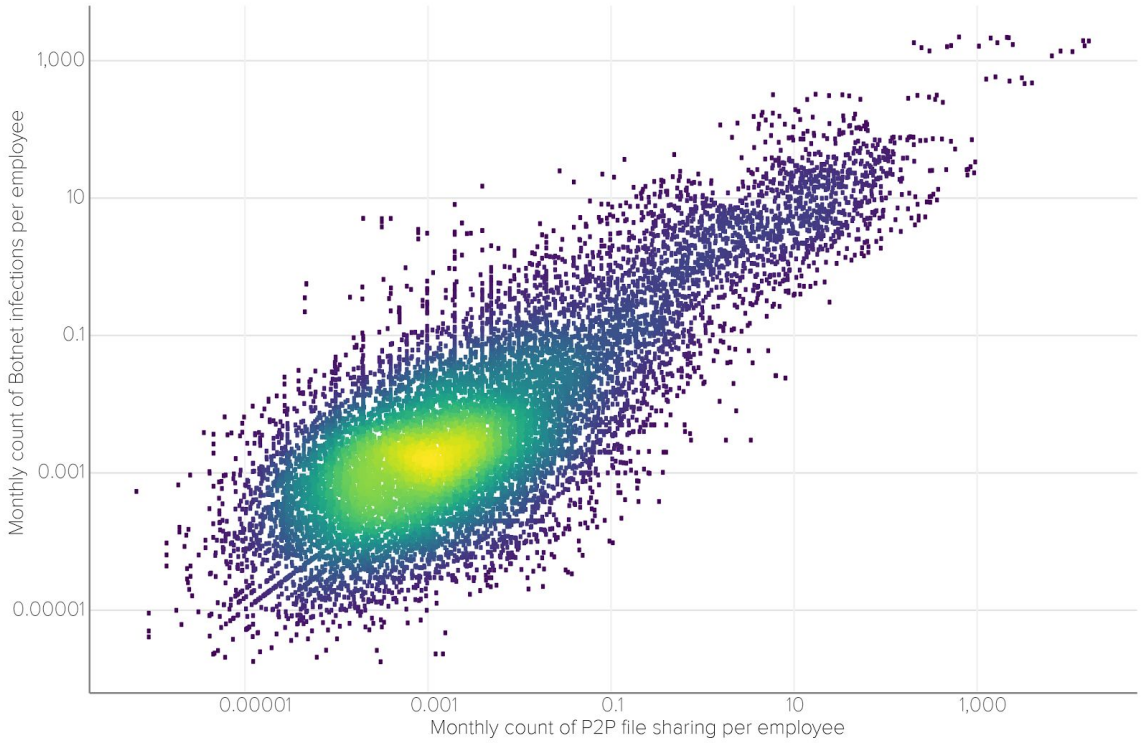
In recent years, government policymakers and regulators have adopted new cybersecurity initiatives in various countries (including the U.S.) without the benefit of quantitative data or metrics to measure success. Security Ratings provide organizational and sector-wide data and metrics to inform policymakers and regulators about the success of past initiatives and offer a quantitative methodology upon which to base or to measure future initiatives.




*Source: "BitSight Insights - Are Energy and Utilities at Risk of a Major Breach?" (2015)*

### c) How User Behavior Affects The Security Posture of Organizations

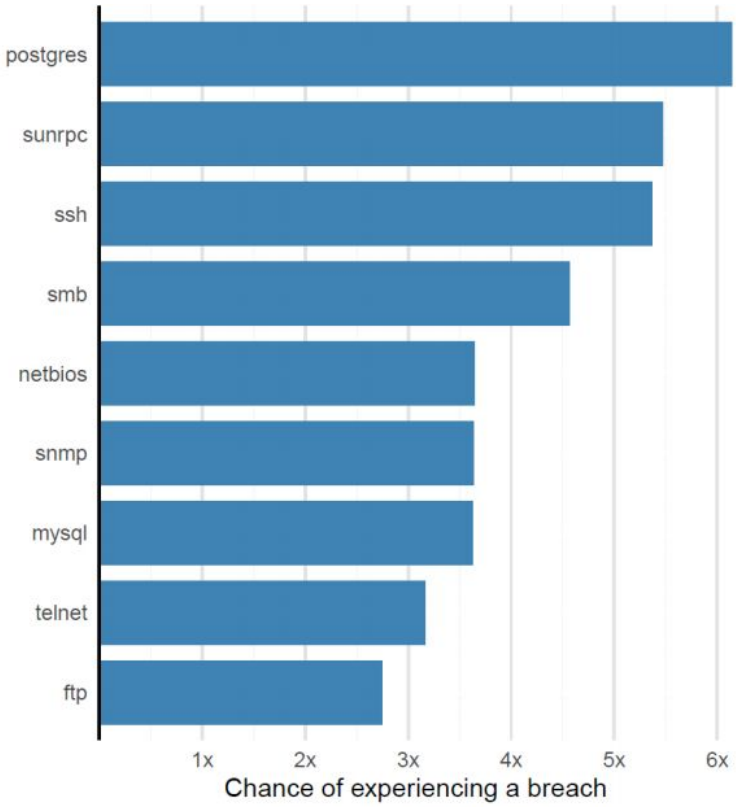
The online habits of employees can have enormous implications on the security posture of organizations. BitSight has studied how peer-to-peer file sharing activity can pose risks to an organization. Researchers found that 43% of applications downloaded using the BitTorrent protocol contained some form of malware. Furthermore, companies with greater peer-to-peer file sharing activity were more likely to have greater incidents of machine compromise on their networks (as shown in the chart below). Policymakers considering adopting new measures to improve security across sectors could conceivably use this data to help prioritize their approaches.




*Source: "BitSight Insights - How Peer-To-Peer Sharing Impacts Vendor Risk and Security" Benchmarking. The X axis is the count of peer to peer file sharing per employee. The Y axis is the monthly count of botnet infections per employee. (2015)*

**d) How The Number Of Services Run Correlate to Data Breaches**

BitSight researchers found that companies that have experienced a publicly-disclosed breach also offer more services exposed to the Internet on average than their non-breached counterparts. Certain services exposed to the internet have a higher risk than others (as seen in the chart below). Again, policymakers considering adopting new measures to improve security across sectors could conceivably use this data to help prioritize their approaches.




*Source: BitSight / Advisen "Cyber Vulnerability: Where Do You Stand?" (2016)*

## (4) Recommendations for the U.S. Government

The Commission will consider a wide variety of recommendations about cybersecurity policy. We hope that the Commission recognizes the value that Security Ratings bring, both as a new and unique data source to help organizations reduce critical third party cyber risk and also as a way to enhance the overall cybersecurity policymaking process with historical and real-time information. To that end, we believe the U.S. government should adopt commercial best practices and begin to continuously monitor critical third party government contractors. We also believe the U.S. government should utilize additional real-time performance metrics in order to hold senior executives and agencies accountable for cybersecurity.

### a) US Government Should Adopt Commercial Best Practice and Begin Continuously Monitor Critical Third Party Vendors/Contractors

Years ago, the U.S. government played a critical role in encouraging both commercial enterprises and government agencies to utilize continuous monitoring technology **to monitor their own enterprises**. In fact, the newest FISMA law enacted in 2014 shifted the focus of agencies away from policy-based reporting to continuously monitoring specific threat, incident,

and compliance information. The latest Office of Management and Budget (OMB) report to Congress on FISMA reveals that continuous monitoring systems are being widely adopted throughout the government for internal monitoring: a large number of agencies now have continuous monitoring programs in place.

**However, while the commercial sector is extensively adopting the concept of continuously monitoring third party vendors, many government agencies have not considered expanding continuous monitoring to include their critical third party contractors.** As evident in the breaches discussed earlier, third party vendors can pose significant risk to organizational security. There are tens of thousands of third parties hold sensitive data or perform services on behalf of the government. Establishing continuous assessment of critical vendors is an important initiative for the government to get a better handle on its own data risk.

We encourage the Commission to recommend that government organizations and agencies utilize high quality, commercially accepted methods, tools, and practices to continuously monitor the cybersecurity effectiveness of critical third party organizations, including vendors, business associates, contractors, subcontractors, critical infrastructure owners/operators, and others. Continuous monitoring tools complement traditional, qualitative security assessments and enable organizations to trust, but also verify the cyber risks associated with third parties. Using the data obtained from continuous monitoring, government agencies can better manage cyber risk across tens of thousands of third parties that would otherwise be impossible to observe.

### b) Utilize Data-Driven Cybersecurity Metrics and Real-Time Reporting to Hold Government Agencies and Senior Leaders Accountable for Cybersecurity and Assess the Effectiveness of National Cybersecurity Policies

The U.S. government must incorporate additional cybersecurity metrics into its policy environment in order to make the best decisions with the best information.

Today, Chief Information Security Officers in large multinational businesses are able to provide cybersecurity metrics and measurements to senior executives in real time, in part by using Security Ratings. Board members regularly consume these metrics during quarterly meetings. They know their jobs are on the line if the company does not execute properly on its cybersecurity initiatives.

The same kind of accountability and responsibility must also exist at U.S. government agencies. To help usher in that system, the U.S. government must improve its data collection and metrics system.

First, the government needs to modernize its data collection process by having the Office of Management and Budget (OMB) move toward automated reporting of agency data in order to continuously evaluate the effectiveness of agency cybersecurity programs. Today, the OMB

relies on an antiquated collection process that prevents it from providing more frequent updates to members of Congress. Without more frequent measurements, it is hard for senior agency officials and members to conduct robust oversight. Having an automated collection process is critical to ensuring that policymakers have the most accurate, objective data possible.

Second, the government must create more useful metrics to better evaluate the effectiveness of an agency's program. Some metrics that the government uses to evaluate agencies are not terribly useful in assessing the security effectiveness of an agency. For instance, in the category of "Malware Defense," agencies are judged on whether they have deployed intrusion prevention and antivirus technology.[1] But what if the technology is deployed, but improperly configured? This could leave the network unprotected. Similarly, the report cites as a strong metric that "100% of agencies completed Indicators of Compromise scans by July 31, 2015."[2] While these scans are certainly a best practice, a better performance metric would have focused on how many machines were fixed after compromise was identified.

Better metrics exist. Most experts agree that measuring the time from initial breach to detection/resolution is the most important and relevant cybersecurity metric. This one metric measures an organization's capability to identify, detect, respond and recover. Many private-sector security professionals use this "golden" metric in board-level reporting. The Obama administration recently listed breach detection and incident response time as one of its five priorities for cybersecurity. Future OMB reports should incorporate these and other "timeliness" metrics in order to truly evaluate an agency's performance.

Finally, in recent years, government policymakers and regulators have adopted new cybersecurity initiatives without the benefit of quantitative data or metrics to measure success. Security Ratings contain organizational and sector-wide data and metrics to inform policymakers and regulators about the success of past initiatives and offer a quantitative methodology upon which to base or to measure future initiatives.

---

[1] Office of Management and Budget, *Annual Report to Congress: Federal Information Security Management Act,* March 18,2016, p.27. Available at: https://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/final_fy_2015_fisma_report_to_congress_03_18_2016.pdf

[2] Office of Management and Budget, *Annual Report to Congress: Federal Information Security Management Act,* March 18,2016, p.6. Available at: https://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/final_fy_2015_fisma_report_to_congress_03_18_2016.pdf

## (5) Conclusion

Security Ratings have become an important foundation for many business relationships where third party cyber risk is a critical factor. The U.S. government can learn a great deal from the successful adoption of Security Ratings and other continuous monitoring solutions. Furthermore, Security Ratings can be tremendously helpful to U.S. government policymakers, providing quantifiable, real-time, actionable information to help policymakers understand the current state of national cybersecurity, measure cybersecurity performance among different sectors and government agencies, assess the impact and effect of previous national policies on sector-wide performance, make data-driven decisions about future cybersecurity policy, and hold accountable government departments and agencies.

BitSight would be happy to provide any additional data and research for the Commission and its members at request.