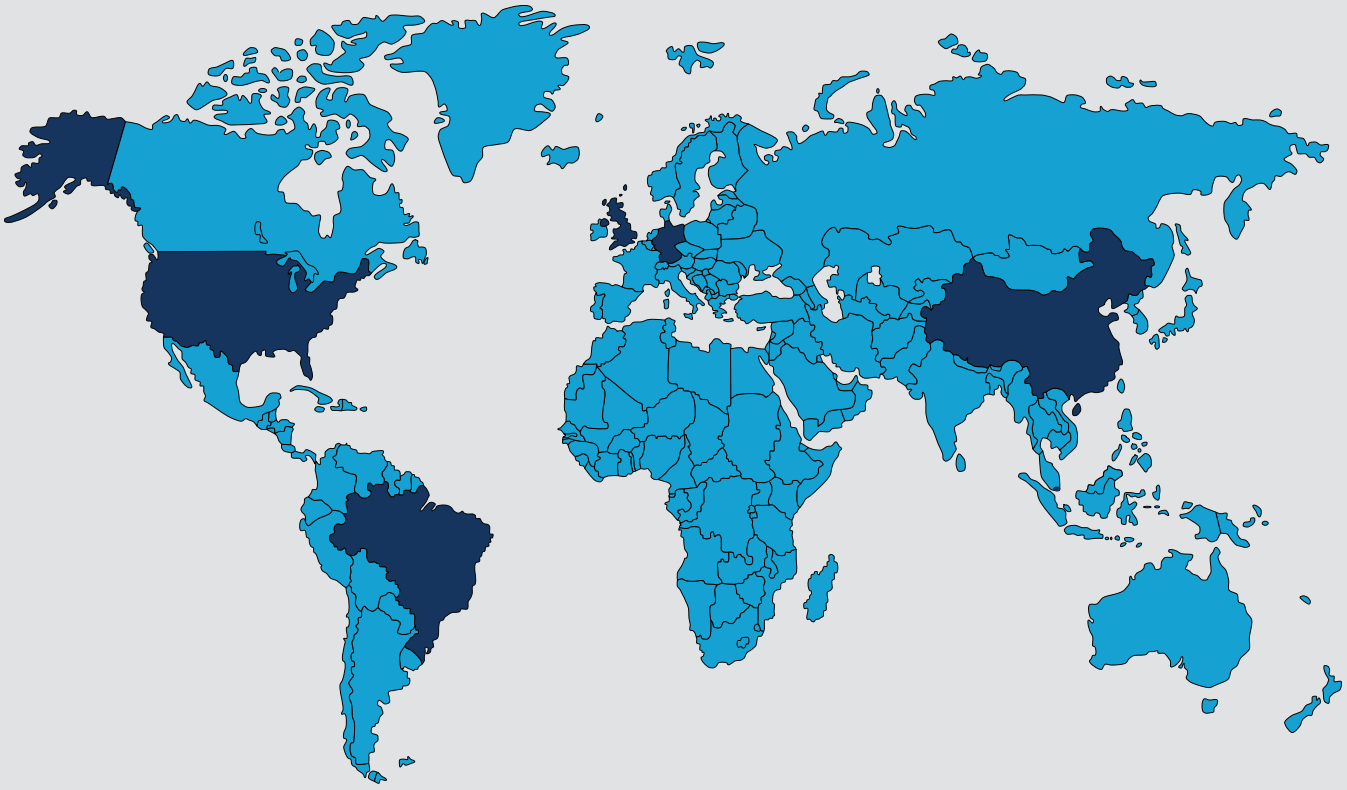
BitSight Insights Global View

Revealing Security Performance Metrics Across Major World Economies



BITSIGHT®
The Standard in SECURITY RATINGS

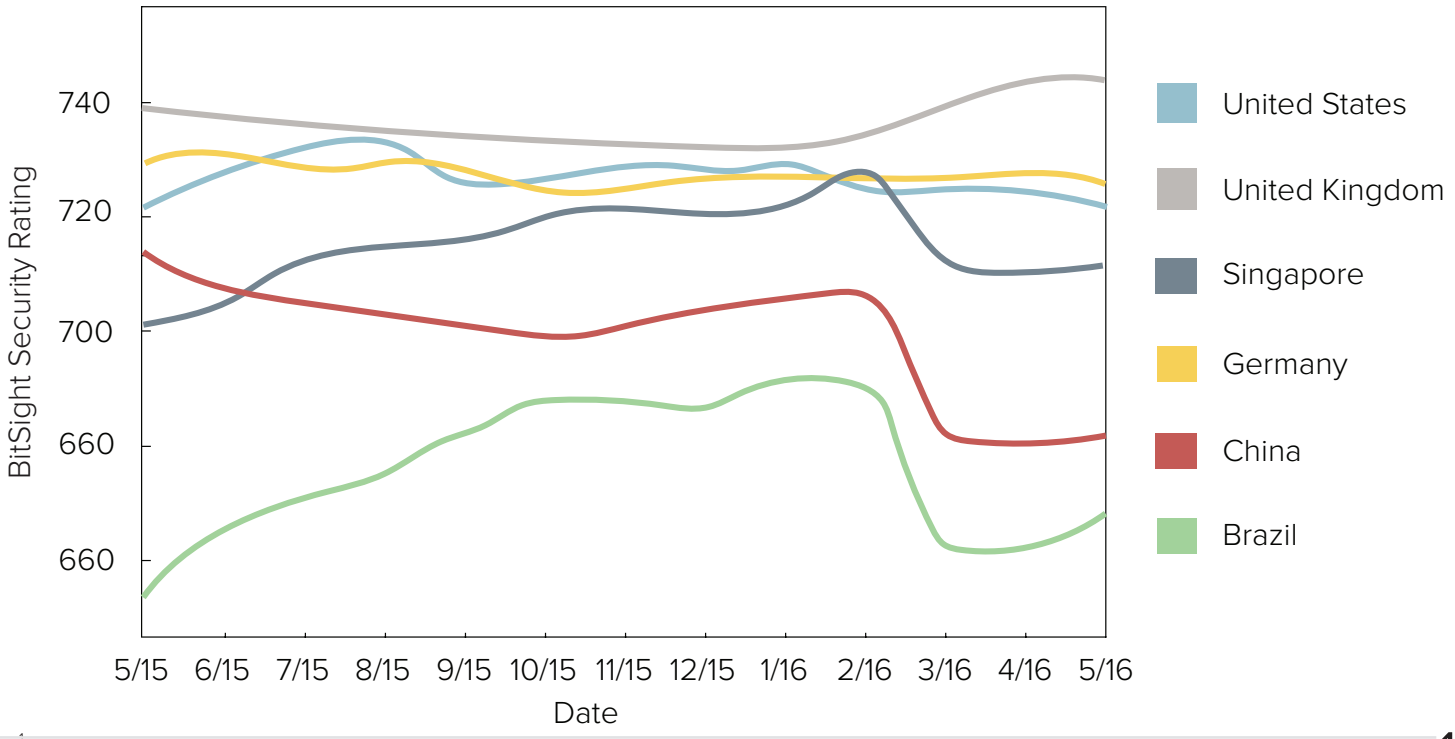
Introduction

There is no denying the global nature of 21st century business. The export and import of goods and services has become a defining feature of the world economy. Germany, the largest European economy by size, derives 45.7% of gross domestic product (GDP) through exports alone[1]. Businesses have embraced this economic globalization and have expanded operations across the globe. Yet, entering new countries can pose financial, operational and legal risks to an organization. Business laws or practices can widely differ between countries and contracting local vendors can introduce new risks to an organization, including cyber risk.

BitSight researchers analyzed the security performance of a random sample of 250 companies per country from the United States, the United Kingdom, Singapore, Germany, China and Brazil. (See Methodology section for more details). Country of origin was determined if greater than 50% of the organization's network assets were attributed to that country. This provides a clear picture of companies that hold the majority of their internet connected technology assets within one of these countries, although it may not reflect more traditional definitions of country origin such as headquarter location. This report analyzes the security performance through metrics that are key components of Security Ratings, such as machine compromise rates, SSL vulnerabilities, peer-to-peer file sharing and email security protocols and more.

The chart below highlights the median BitSight Security Rating of companies in these countries from May 1, 2015 to May 1, 2016. It becomes apparent that Germany, the UK and the US are top performers. The United Kingdom, the country in our sample that ended with the highest median security rating, started the year at 737 and ended at 740. German companies started the year at 728 and ended the year at 725. The United States has similar ratings to Germany, starting at 721 and ending at 720. Singapore was a middle-of-the-pack performer that started at a 701 and ended the year at 711. The dip in ratings for Singapore, China and Brazil starting at the beginning of February can be attributed to the addition of two risk vectors - File Sharing and Open Ports - within BitSight's algorithm. China saw a downward trend in performance, beginning the year at 712 and ending at 683. Lastly, Brazil has significantly poorer performance than the other countries included in the study. Brazilian companies had a median rating of 653 on June 1, 2015 and ended at 666 on June 1, 2016. Companies in Brazil also suffered from a higher rate of compromised machines and file sharing activity in comparison to the other countries.

Median BitSight Security Ratings of Companies in Major World Economies



[1]All economic data in this report is from the World Bank website: http://data.worldbank.org/
Note: Margin of error for median ratings is +/-10 points

Key Findings

1. Companies based in Brazil have the lowest aggregate Security Rating while companies in the UK, Germany and the US have the highest.

2. Brazil and the United States have the poorest performance when it comes to preventing and mitigating botnet infections; Germany and the UK perform the best in the fight against botnets.

3. Major SSL vulnerabilities such as Heartbleed, POODLE and FREAK continue to affect organizations within all countries included in the study.

4. Peer-to-peer file sharing is common across all countries included in the study, except Germany.

5. China, Brazil and Germany have a higher percentage of poorly configured email security protocols, such as SPF and DKIM.

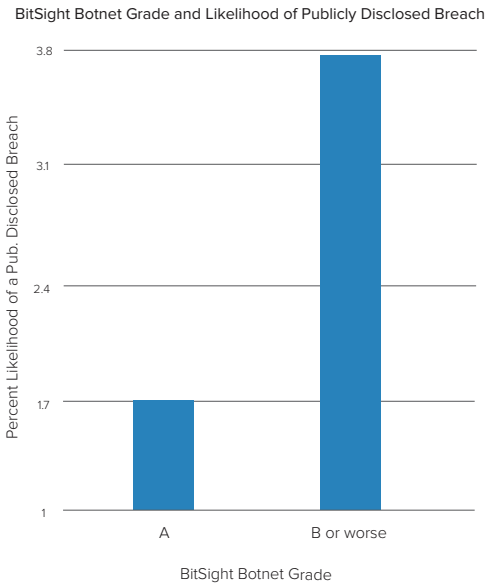
About BitSight

BitSight is the worldwide leader in providing objective, accurate and actionable Security Ratings to organizations around the world. BitSight Security Ratings are a measurement of an organization's security performance. Much like credit ratings, BitSight Security Ratings are generated through the analysis of externally observable data. Leading companies, including the top private equity firms, largest banks, major insurers and more are leveraging these ratings to mitigate vendor risks, underwrite cyber insurance, benchmark security performance, perform M&A due diligence and manage portfolio cyber risk.

Machine Compromise Activity

Companies in Brazil have a higher rate of compromised machines on corporate networks

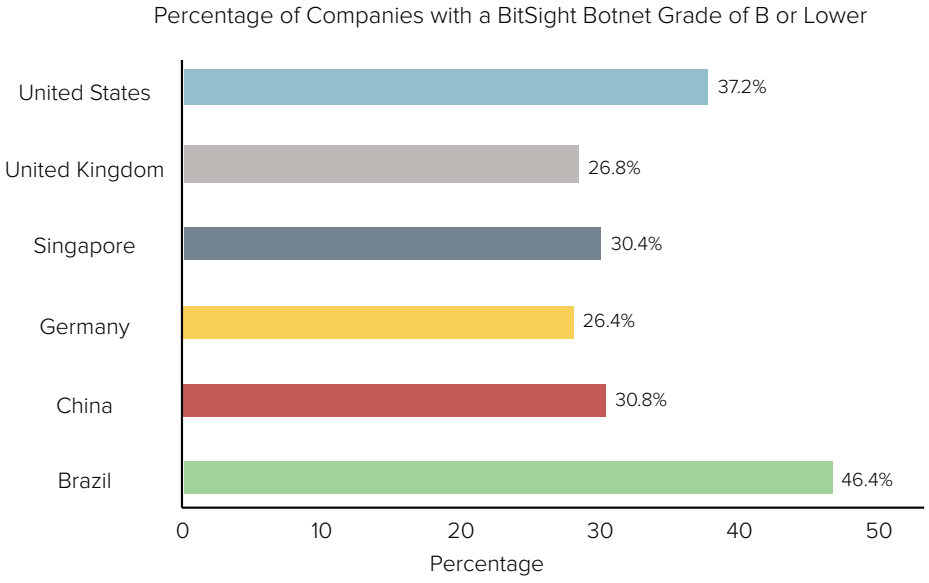
Botnets are networks of computers that have been compromised or infected with malicious software and controlled as a group by an adversary without the owners' knowledge. These infections are direct evidence that an outside attacker has gained access and/or control of a system. But beyond access to a corporate network, companies with poor performance in protecting and eliminating botnets have led to other major problems.



In 2015, BitSight undertook a study to understand the correlation between botnets and publicly disclosed data breaches. Within a sample of 6,273 companies[2], **BitSight researchers found that companies with a BitSight botnet grade of "B" or lower were more than twice as likely to experience a publicly disclosed breach**. BitSight botnet grades are a component of the overall Security Rating of an organization. These grades indicate the performance of an organization in preventing botnet infections and mitigating events that do occur quickly.

Looking within our sample of 250 companies per country, it becomes apparent that botnets are an issue for companies within all countries. A bright spot here is the fact that the majority of organizations have "A" grades within the countries analyzed; this indicates that companies have either no botnet infections, or they have few infections and are quick to address them.

Nevertheless, some countries are performing poorer than others[3]. Almost half (46.4%) of Brazilian companies had a grade of "B" or lower, significantly higher than UK, Singapore, Germany and China. Symantec noted in 2010 that Brazil accounted for 41% of spam botnets in Latin America and 7% worldwide[4]. Brazil was also the country with the lowest Security Rating throughout the past year. Brazil has documented challenges with malware. For example, Microsoft noted in a recent report that Brazil's encounter rate - the percentage of computers running Microsoft security products that report a malware encounter - was 65% higher that the worldwide average in the second half of 2015[5].



The United States had 37.2% of organizations getting a grade of "B" or lower, while the UK, Singapore, Germany and China all had between 26.4 to 30.8% of companies falling in this range. As earlier BitSight research suggests, companies with botnet grades that are below an "A" are more likely to have serious cyber events, primarily publicly disclosed breaches. As organizations look to expand internationally, whether expanding technology infrastructure or outsourcing services to a third party provider, botnets should be a top concern on which to focus.

[2]Download BitSight's 2015 botnet report here: https://info.bitsighttech.com/insight-report-breach-botnet
[3]All percentages represent data from May 1, 2016.
[4]http://securityresponse.symantec.com/threatreport/topic.jsp?id=lam&aid=lam_countries_of_botnet_spam_origin
[5]https://www.microsoft.com/security/sir/default.aspx
Note: Margin of error for botnet data is +/-6%

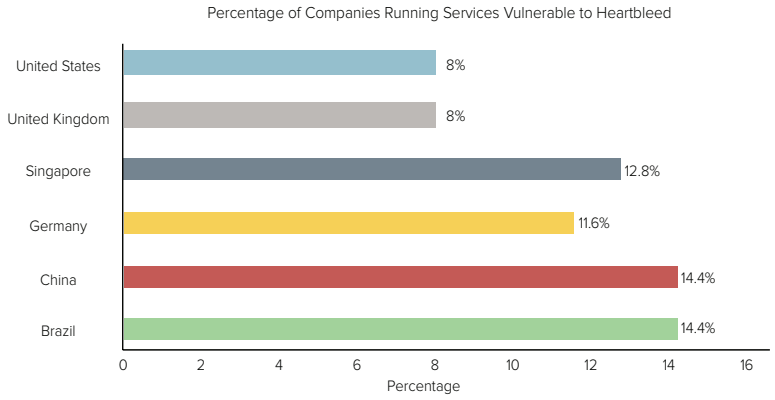
Internet Communication Vulnerabilities

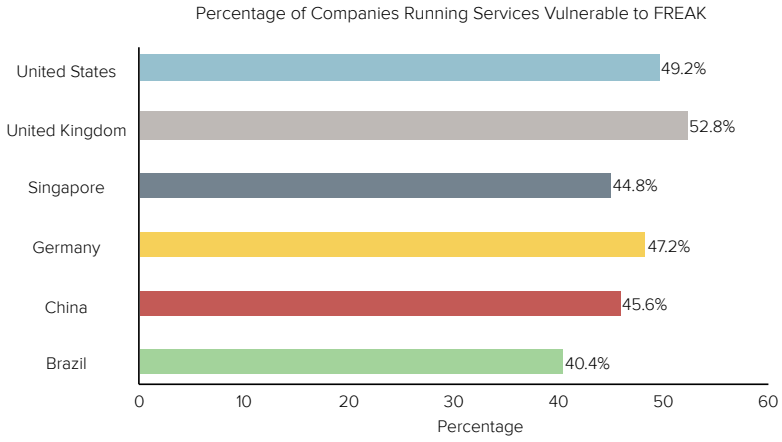
All countries can improve on remediation of vulnerabilities in important internet communication protocols

Transport Layer Security (TLS) and Secure Sockets Layer (SSL) are widely used protocols to secure communications over the internet[6]. SSL/TLS vulnerabilities such as Heartbleed, POODLE and FREAK are were major news stories when they first were uncovered. Heartbleed, the first and likely most well-known SSL vulnerability, was first announced in April 2014. This vulnerability made it possible for an attacker to trick systems into revealing information such as login credentials, cookies and more. Heartbleed was not only fodder for the news media: in August 2014 it was revealed that the massive breach of 4.5 million patient records at Community Health Systems was a result of the Heartbleed vulnerability on a system that was exploited by attackers[7].

POODLE, announced in October 2014, involved an SSLv3 vulnerability that could allow attackers to perform a man-in-the-middle attack to steal information. Not long after, FREAK was announced in March 2015. This vulnerability allows attackers to "decrypt security communications between vulnerable clients and servers.[8]" Despite the high profile nature of these vulnerabilities, BitSight observed a high percentage of companies across the globe running services vulnerable to Heartbleed, POODLE and FREAK[9].

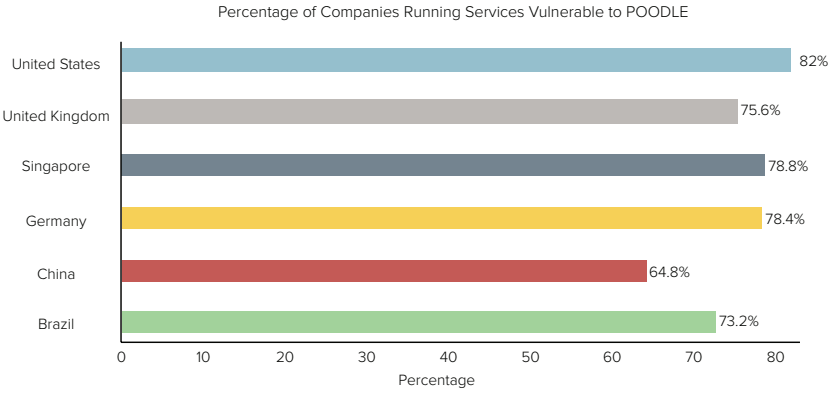
Heartbleed is the least prevalent of the SSL vulnerabilities. Within our sample, the UK and the US had 8% of companies running services vulnerable to this bug. Germany had 11.6% of companies and Singapore had 12.8% of companies vulnerable to Heartbleed. China and Brazil both had 14.4% of companies within these two major economies running services vulnerable to Heartbleed.





FREAK is significantly more common than Heartbleed among companies within these six countries. Between 40.4% to 52.8% of companies within these country samples were running services vulnerable to FREAK. Brazil, had the lowest percentage of companies running services vulnerable to FREAK although this finding is not statistically significant in comparison to the other countries.

POODLE is far and away the most prevalent SSL vulnerability, with high percentages of companies within all countries running services vulnerable to this bug. Interestingly, China had a significantly lower percentage than the US, Singapore and Germany. Nevertheless, this finding may be biased by the fact that few companies have employed SSL on their domains in China[10].



[6]For more information on SSL vulnerabilities: Heartbleed: https://www.us-cert.gov/ncas/alerts/TA14-098A; FREAK: https://www.us-cert.gov/ncas/current-activity/2015/03/06/FREAK-SSLTLS-Vulnerability; POODLE: https://www.us-cert.gov/ncas/alerts/TA14-290A
[7]http://www.reuters.com/article/us-community-health-cybersecurity-idUSKBN0GK0H420140820
[8]https://www.bitsighttech.com/blog/poodle-is-back-tls-targeted-by-new-bug
[9]All percentages represent data from May 1, 2016.
[10]See Methodology section for more info
Note: Margin of error for SSL data is +/-6%

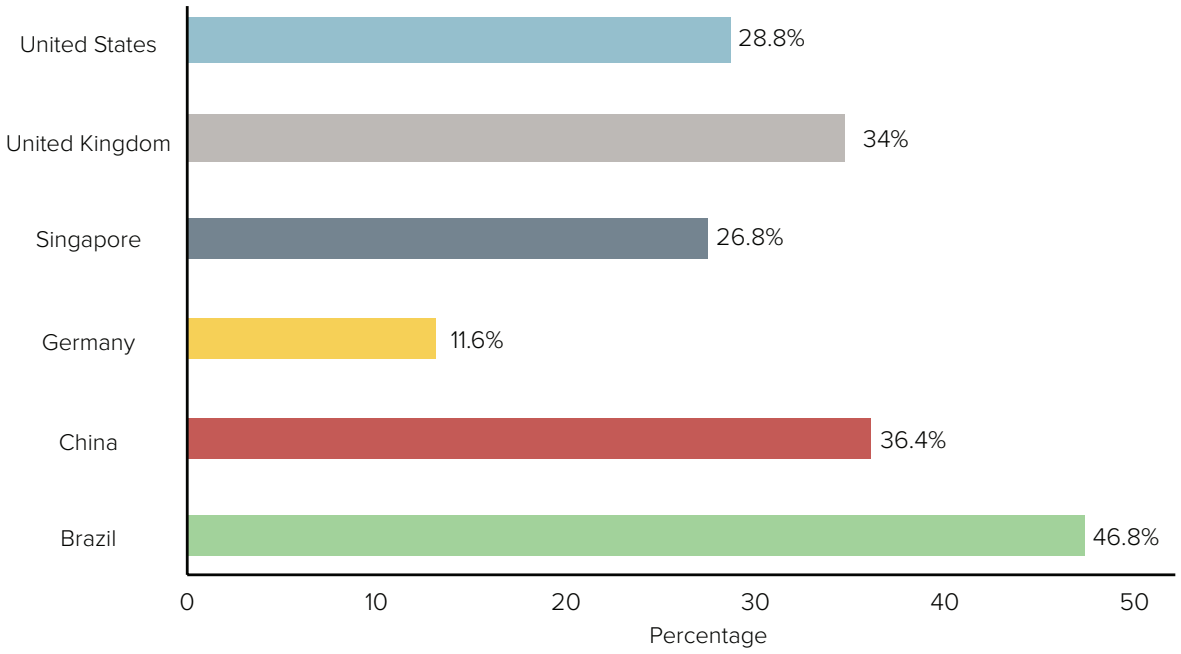
File Sharing Activity

Brazilian businesses have higher rate of harmful peer-to-peer file sharing on corporate networks

Peer-to-peer file sharing over the BitTorrent protocol is a prevalent issue for companies in Brazil. BitSight observed a higher incidence of peer-to-peer file sharing on corporate networks in Brazil, with 46.8% of companies in this country experienced file sharing activity in the past year. Companies in China and the United Kingdom also had a sizable percentage of companies exhibiting this behavior, with 36.4% and 34% respectively. The United States had 28.8% of companies with file sharing activity and 26.8% of Singaporean companies had file sharing on their corporate networks.

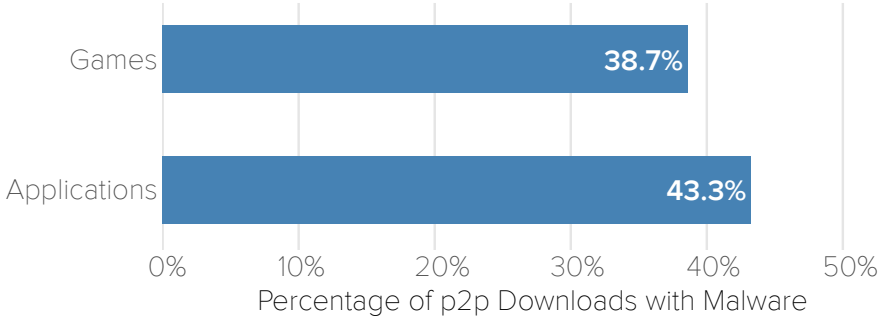
An interesting point of data was the low percentage of file sharing in Germany. German companies had a significantly lower percentage of companies with observed file sharing activity on corporate networks, with only 11.6% of companies showing evidence of peer-to-peer downloads. One potential explanation could be documented enforcement practices in Germany[11], such as fines for those who break the law regarding peer-to-peer file sharing.

Percentage of Companies with File Sharing Activity in the Past Year



Why is File Sharing a risky behavior?

BitSight recently published a report on file sharing behavior on company networks. While file sharing is not an inherently harmful activity, it poses major security risks if employees are unaware of the origin of files that may contain malware. BitSight's Data Science team analyzed a sample of 215 torrented applications and 104 torrented games and found 38.7% of games and 43.3% of applications contained malware.



Download this report here: https://info.bitsighttech.com/how-peer-to-peer-file-sharing-impacts-vendor-risk-security-benchmarking

[11]http://www.zdnet.com/article/file-sharing-in-germany-could-the-cost-of-getting-caught-be-about-to-come-down/

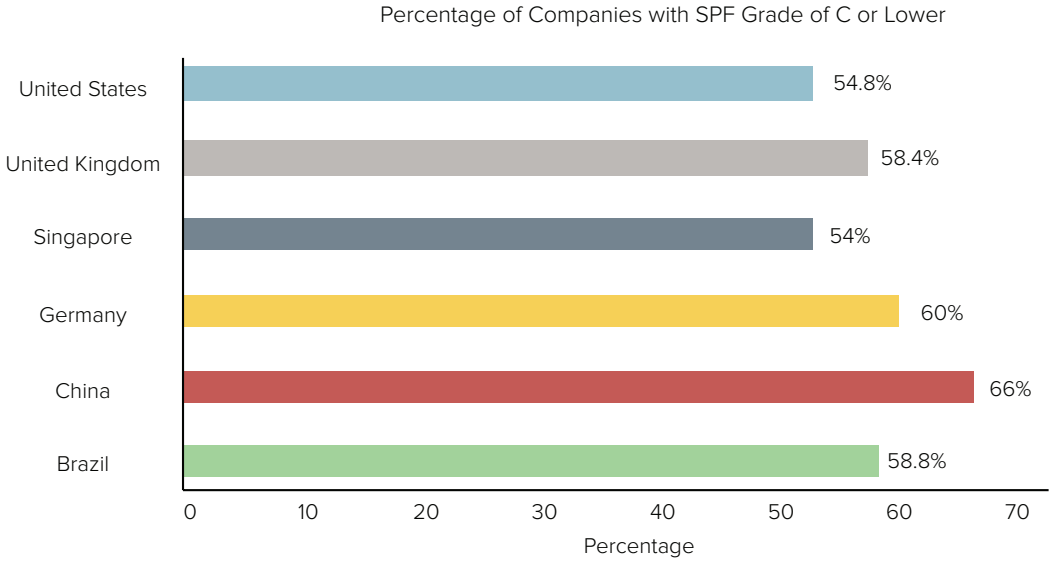
Note: Margin of error for File Sharing data is +/-6%

Protecting Email Communications

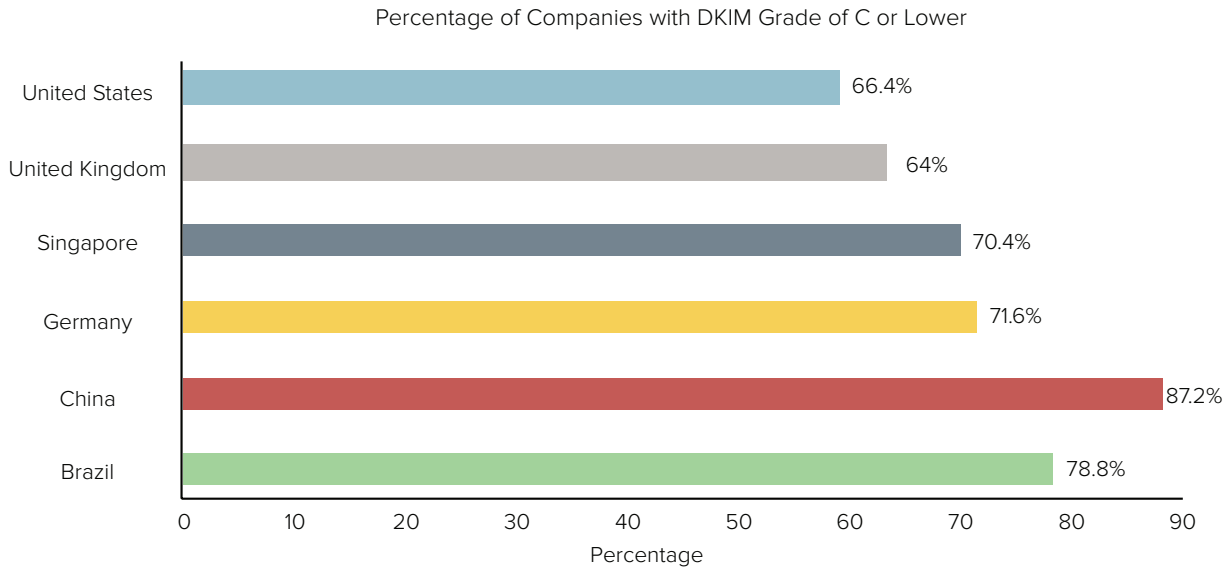
Organizations across all countries can improve adoption and configuration of email security protocols

To gauge the level of email security performance across companies within the sample, BitSight researchers looked at the utilization of two important email security protocols: Sender Policy Framework (SPF) and DomainKeys Identified Mail (DKIM). BitSight researchers specifically looked at the proportion of companies that had a BitSight SPF or DKIM grade of C or lower.

Sender Policy Framework is an important domain name system record that identifies which mail servers are permitted to send email on behalf of a domain. These records help limit an attackers ability to successfully spoof a valid "From" address. Snapchat, the social photo/video sharing platform, recently suffered a breach of employee payroll data when an attacker impersonated the CEO using a fake email address[12]. Within our sample, some countries fared better than others. China had the largest percentage of companies with an SPF grade of C or lower followed by Germany, the United Kingdom and Brazil. The United States and Singapore had a lower percentage of companies with a low grade for implementing SPF.



DKIM is another important email protocol that is designed to authenticate valid servers and limit the sending of spoofed email messages. The graph below represents the percentage of companies with a BitSight DKIM grade of C or lower. Within our sample, China and Brazil had a higher percentage of companies with low grades when it comes to implementing DKIM. Germany and Singapore had 71.6% and 70.4% respectively. The US and UK had a lower percentage of companies with poor performance.



[12] http://techcrunch.com/2016/02/29/snapchat-employee-data-leaks-out-following-phishing-attack/

Note: Margin of error for SPF and DKIM data is +/-6%

Recommendations for Businesses

All business relationships carry inherent levels of risk. As these relationships begin to expand across the globe, new risks have emerged, including cyber risks. Sharing sensitive data with global partners and vendors is important for conducting business efficiently but risk managers and security professionals should be aware of potential cyber risks that may arise across borders. BitSight recommends that security and risk professionals take the following steps to mitigate vendor risks across the globe:

1. **Put clear agreements in place about the storage and use of your corporate data.**

   Understand where the data will be stored and what level of access a vendor's employees have to data. Ask about encryption of data and policies around proper usage of company data.

2. **Create standards of security performance for global vendors and partners.**

   Implement service level agreements (SLA) for the security performance for all vendors. Utilize a continuous monitoring tool to objectively understand all vendors' security performance. Create an action plan to enable vendors to remediate issues identified on their network.

3. **Understand global security trends and potential risks of doing business in a given country.**

   Evaluate the potential security risks of doing business in a particular part of the world. Understand laws and regulations surrounding cyber security practices. Analyze aggregate trends of company performance in other parts of the world.

Methodology

For this study, BitSight researched selected 250 entities from each of the six countries out of our set of 47,500+ entities. To be eligible for selection, an organization needed more than 50% if its IPv4 addresses mapped to the country in question. Companies were also excluded if the known employee count was less than 1000. We used data collected by Bitsight over the period May 1, 2015 to May 1, 2016.

In order to gain an accurate view of security performance, BitSight collects network asset information utilizing a team of technical researchers. By compiling this information, BitSight is able to collect publicly accessible information on a wide range of security metrics and assign it to a specific organization. BitSight collects data from a wide variety of reputable sources, including from our threat intelligence subsidiary AnubisNetworks, and other respected and trusted data sources. BitSight is committed to providing the most accurate and actionable data to power our ratings.

One potential bias that may exist in this report is in relation to SSL data in China due to the lack of adoption among Chinese organizations. BitSight researchers found the Chinese SSL results are biased but represent a lower limit on the presence of various vulnerabilities.

Conclusions

As organizations continue to extend operations globally, the findings of this report are relevant for stakeholders across the enterprise. Along with operational, financial and legal risks, cyber risk poses a challenge to the global business. Security and risk professionals can leverage the recommendations within this report for multiple use cases:

1. **Manage Global Vendor Risks**
   Identify aggregate security trends in a vendor's country. Continuously monitor global vendors and have an action plan in the case of a major security lapse, such as a growing botnet infection. Verify that global vendors are preventing risky behaviors, such as file sharing, and are properly configuring and maintaining standard security protocols.

2. **Underwrite Cyber Insurance for Global Organizations**
   Identify security issues in different parts of an organization's global network. Understand potential risks to underwriting businesses with technology assets in a particular country. Ask questions about data sharing between global components of multinational businesses.

3. **Benchmark Security Performance of Global Networks**
   Implement continuous monitoring for network components that are overseas. Understand the potential risks to implementing technology infrastructure in another country and monitor key performance indicators, such as time to remediate botnets and other serious infections.

4. **Conduct Global M&A Due Diligence**
   Identify an acquisition target's performance relative to peer companies in their home country and industry. Analyze issues on the company's network and enable them to remediate major issues. Continuously monitor the performance of the company through the acquisition and beyond.

BITSIGHT

ABOUT BITSIGHT TECHNOLOGIES

BitSight Technologies is a private company based in Cambridge, MA. Founded in 2011, BitSight Technologies provides businesses with daily security ratings that objectively measure a company's security performance to transform the way they manage risk.

For more information contact us at:

BitSight Technologies
125 CambridgePark Drive
Suite 204
Cambridge, MA 02140

www.bitsighttech.com | sales@bitsighttech.com