Cyber Security Myths Versus Reality:
How Optimism Bias Contributes to Inaccurate Perceptions of Risk

June 2015
Introduction

Cyber risks continue to pose a major threat to businesses across all industries. The 2015 Verizon DBIR report found that there were nearly 80,000 security incidents observed across all industries. In addition, 70% of attacks affect a secondary victim, such as a third party or vendor. With increased incidents and exposure, board directors and executives are taking note of cyber security as a strategic issue. A recent survey from consulting firm BDO International found that 54% of board directors are more involved in cyber security today than one year ago. As companies continue to face new threats against their information assets, it becomes increasingly important for organizations to answer the fundamental question: Is my organization secure?

While it is impossible to guarantee absolute security, benchmarking performance against peers and industry averages can provide visibility to an organization’s performance relative to others. This intelligence can be leveraged across the enterprise, from making tactical decisions within the security team to strategic C-level decisions on investments, initiatives and hiring for cyber security. Without the ability to benchmark performance, businesses can suffer from optimism bias. Optimism bias refers to an overestimation of the likelihood of positive outcomes or an underestimation of the likelihood of negative outcomes. When it comes to IT security, optimism bias can lead to decision making based on an unrealistic understanding of cyber risks facing an organization. Without reliable information businesses are at a major disadvantage to effectively undertake the following initiatives:

- Reporting to the Board about cyber security
- Filling out or assessing vendor questionnaires
- Conducting Mergers and Acquisitions due diligence
- Making informed decisions about security strategy

BitSight Technologies provides organizations worldwide with data-driven security ratings to quickly and objectively measure cyber risk. Much like credit ratings, BitSight Security Ratings are generated through the analysis of externally observable data. Armed with daily ratings, organizations can better manage third party risk and benchmark their security performance, providing answer to the question of whether we are more or less secure than our peers, competitors and partners.

BitSight commissioned a study with Dimensional Research, a leading market research firm, to survey IT professionals about their organization’s performance relative to industry peers across a wide range of cyber security controls. The study indicates that IT professionals demonstrate significant optimism bias about the performance of their organization’s cyber security practices in relation to industry peers. While only 6% of survey respondents said their organization fell into the lowest performance tier of Basic, BitSight data indicated that close to a quarter of companies fell into this Basic category. On a wide variety of questions, survey respondents both over- and underestimated their performance in relation to industry peers. Without standard metrics and comparative data points, many businesses appear to be lost at sea when it comes to measuring their security program’s effectiveness.
To undertake this analysis, Dimensional Research surveyed 331 IT professionals from four key industries: Retail, Healthcare, Financial Services and Energy/Utilities. Respondents were IT executives (48%) or IT team managers (58%) working within organizations of 500+ employees. The survey consisted of questions that asked IT professionals to rate themselves as Advanced, Intermediate, or Basic in comparison to their industry peers on a variety of cyber security controls and practices.

BitSight compared these survey results with quantitative data on the cyber security performance of 4,157 companies. This data set included companies with 500+ employees within the Retail, Finance, Healthcare and Energy/Utility sectors. Using its outside-in approach to gathering and processing data, BitSight is able to assign a top-level security rating as well as letter grades (A-F) to organizations based on their relative performance on a wide array of risk vectors. In order to compare these letter grades to the survey questions, the letter grades have been divided into three corresponding categories:

- A Grade: Advanced
- B and C Grades: Intermediate
- D and F Grades: Basic

BitSight provides quantitative, data-driven Security Ratings to organizations worldwide. Security Ratings range between 250 and 900, with higher ratings indicating better performance. They are calculated using terabytes of data, including nearly 4+ years of historical information on risk vectors, by using a proprietary algorithm. Risk vectors include security events, which are observed compromises on a company’s network, and diligence risk vectors, which show steps a company has taken to prevent attacks. For each risk vector, an overall letter grade (A-F) is assigned, indicating the company’s performance relative to others. The grade takes into account factors such as frequency, severity, and duration (for events) as well as record quality, evaluated based on industry-standard criteria (for diligence).

Using both automated and hand-curated tools and processes, BitSight creates comprehensive network maps of a company’s Internet footprint. These maps allow BitSight to determine the organizational origin of compromised devices belonging to tens of thousands of companies across the globe.

When asked about their company’s overall security performance, a majority (57%) of respondents rated themselves as Intermediate. Interestingly, many respondents either over- or underestimated their performance relative to others. For example, only 6% of respondents believed their company was in the Basic category. BitSight data suggests 24.6% of companies fall into this lowest performance tier.
Looking at a breakout of the industries surveyed, we can see markedly different perceptions of performance between sectors. Finance, for example, is much more confident about their performance than the other surveyed industries - and rightfully so. As an industry, they are the highest performer with BitSight rating 54% of companies within the Advanced category. Yet, a clear optimism bias does emerge at the lower end of the industry: only 3% surveyed would rate themselves in the Basic category, but BitSight data finds around 14.6% of Finance companies fall here.

The other three industries show a similar pattern to Finance: Most respondents perceive themselves in the middle, with fewer indicating themselves as Basic or Advanced performers. The largest disconnect between BitSight’s rating of an industry and the survey respondents occurs within Healthcare. Only 7% of respondents in the Healthcare sector rated their performance as Basic, while BitSight data suggests 37.5% of companies fall into this category. This industry has been hit by major breaches affecting customer data, including Anthem Health and Community Health Services, in the past few months.

In every industry, fewer respondents indicated they fell into the Basic category than BitSight data suggests. On the other end of the spectrum of high performance, perception and reality are more aligned in the Finance, Healthcare and Retail industries. For the Advanced category, these industries had <=5% difference between survey respondent’s perception and BitSight industry data. On the other hand, the Energy/Utilities sector appears to suffer from a lack of confidence among top performers. Fourteen percent of respondents indicated their organization’s performance fell into the Advanced category of cyber security performance. In contrast, BitSight industry data shows 35.2% of companies are rated in this category. This likely means that IT professionals may underestimate their organization’s cyber security performance in relation to others.

Looking at aggregate and industry trends, it becomes increasingly apparent that companies are struggling to fully grasp their level of performance in relation to industry peers. Without establishing a baseline of performance, it is difficult to drive strategic decision making on cyber security issues within the enterprise.

**Despite Headlines, Organizations Are Still Exposed to Major Security Flaws**

Heartbleed, Shellshock and FREAK all captured headlines this year as major security vulnerabilities that could compromise the secure flow of information across the Internet. So what about IT professionals’ perception of their organization’s’ vulnerability to these major bugs?
When asked whether encrypted services were updated to address recent vulnerabilities such as Heartbleed, POODLE and FREAK, 80% of respondents indicated their organizations were protected. BitSight performed an analysis on the four industries surveyed and found that while very few were vulnerable to Heartbleed, the other two vulnerabilities still largely affect these industries. More than 70% of companies across these industries were still vulnerable to POODLE. For FREAK, a sizeable portion of companies in these industries (38-51%) are still susceptible to this vulnerability.

Interestingly, when it comes to third parties, only 12% of respondents indicated they were “not confident” in their third party vendors’ patching process to protect against these vulnerabilities. Looking at the BitSight data, it is abundantly clear that many businesses - including vendors that may have access to critical data - are not effectively patching systems against major bugs and vulnerabilities.
Poor Email Configurations Leave Organizations Vulnerable to Attack

Ensuring proper email configuration is a key method for preventing spoofing and phishing attacks against the enterprise. These attacks have become an increasingly common way for hackers to target specific companies with the goal of gaining credentials to access a company’s sensitive data. Recent high-profile breaches such as Anthem and JPMorgan Chase originated from phishing schemes, highlighting the importance of email configurations.

Generally, companies believe they are effective in this area. In this survey, 86% respondents said they had implemented industry standard email configurations to limit attacks. BitSight analyzed specific types of configurations to see if companies were implementing industry standard controls to prevent these attacks. Sender Policy Framework (SPF) is a DNS (Domain Name System) record that identifies which mail servers are permitted to send email on behalf of a domain. SPF records help prevent spammers from sending emails with forged From addresses. Although unconfirmed, there are reports that the Anthem breach was directly related to a phishing attack, potentially caused by poor email security practices. When surveyed about SPF records, 57% of respondents indicated that they ensured proper configuration. Yet, BitSight analysis of the surveyed industries paints a different picture: we found that 68.3% of companies do not have SPF records configured to industry standards. This could mean that SPF records configured allow a large number of hosts, are not syntactically correct, or that they do not exist at all.
Another important configuration is DomainKey Identified Mail (DKIM). These records are important to prevent email spoofing by preventing unauthorized servers from sending email on behalf of a domain. BitSight assesses whether or not companies have DKIM records for each domain that they own, as well as the level of encryption for each configured record. In this survey, 44% of respondents said that they had properly configured DKIM Records. However BitSight analysis shows that an overwhelming 98.2% of companies have DKIM records with low levels of encryption, or do not have DKIM records in place for any of their given domains.

With many high-profile data breaches originating from email, the contrast between perceived performance and actual performance should be a serious concern. The majority of companies overrate their own configuration and implementation of SPF and DKIM records, indicating that companies are not accurately measuring their security effectiveness in this area. Also noteworthy is the confidence given to third parties’ implementation and configuration of SPF and DKIM records. Of those surveyed, 71% expressed a degree of confidence that third parties were meeting industry standards. This percentage contradicts the findings above, which show that a large majority of companies represented in the survey do not have records configured to industry standards.

Security events affecting a company’s network can lead to major issues - including large scale data breaches. BitSight defines these security events as evidence of system compromise. Such security events can include major infections, including malware, botnets\(^1\), and potentially unwanted applications (e.g. adware or grayware) observed on a company’s network. A joint study between Microsoft, IDC, and the University of Singapore estimated that enterprises will spend $127 billion dealing with security issues as a result of malware from pirated software and file sharing.

\(^1\) To learn more about BitSight collection of botnets and how they are correlated to significant publicly disclosed breaches, download BitSight’s previous Insights report, “Beware the Botnets: Botnets
When surveyed about their organization’s ability to detect and respond to systems compromised through malicious code, many respondents are unaware of their organization’s performance. **A mere 8% of companies believe that they fall into the Basic category when it comes to detecting malicious code.** BitSight data demonstrates that within these industries, a much larger percentage of companies (25.5%) are failing to detect malicious code on their networks.

Looking at PUAs’s, the majority of respondents classified themselves as being in the middle third of companies in their industries for having advanced controls to prevent installation on corporate devices. Dimensional Research Data showed that 56% of respondents ranked themselves as Intermediate. However, BitSight data on these industries showed that just 32.5% of companies were in fact intermediate.

Similar to other questions around performance, survey respondents either over- or underestimated their performance when it comes to preventing PUAs’s on their networks. As an aggregate, 32% of respondents classified themselves as having Advanced controls relative to peers in their industry. BitSight industry data suggests that 48.8% of companies within these four industries are Advanced. A similar pattern emerges with the Basic category: Dimensional Research data showed that 12% rated themselves as basic, where BitSight industry analysis shows 18.7% of companies falling into this category. A breakout of the industries also uncovers a similar pattern.

**Conclusion: Organizations Can Overcome Optimism Bias with Continuous Performance Metrics**

This analysis has implications for IT decision makers and other stakeholders, including board members and executives. It is clear that IT professionals’ perception of their organization’s cyber security performance across a wide range of important threat vectors does not align with industry data collected by BitSight. In most instances, very few respondents indicated they fell into the lowest tier of performance across various categories. In reality, BitSight data indicated that far more companies are falling below industry standards on important security practices, from detecting malicious code and configuring SPF records to patching against well-publicized vulnerabilities. Without proper knowledge of cyber security performance relative to others, it is difficult to make impactful and informed decisions about security priorities, budget, headcount, and initiatives. By benchmarking performance against industry peers and averages, businesses can begin to arrive at actionable intelligence to inform both tactical and strategic decision making. IT decision makers can also leverage benchmarking performance to accurately and confidently report to the executive board.
Board directors are becoming increasingly involved in the risk management of cyber security issues. While not actively involved in the management of configuration records or events of a company’s network, board members need to be informed of overall security posture of the organization, and in an increasing number of cases, their vendors. Boards and companies are more often being held liable for the protection of sensitive information; just last year the Federal Trade Commission (FTC) filed a lawsuit against Wyndham Hotel Group for failing to take necessary steps to protect customer data. By understanding relative performance benchmarks and being able to track high-level key performance metrics, boards can address these concerns and make informed strategic decisions involving cyber security.

For cyber insurers and third party risk managers, this study has implications about the efficacy of reliance on questionnaires and audits that may produce biased results. While qualitative assessments of controls and processes can be crucial in making decisions, complementing such methods with unbiased, quantitative metrics can help verify control effectiveness. Cyber insurance underwriters can use quantitative ratings and industry averages to better understand and manage the performance of applicants and their current insureds.

Overcoming optimism bias within an organization can be a challenging task. Armed with actionable and data-driven information, security and risk professionals can begin to drive change within their organizations and their extended networks through communication and transparency.

**Glossary**

**Botnet Infections**: Hosts observed participating in a botnet, including active bots and Command and Control servers.

**DKIM**: A protocol designed to prevent unauthorized servers from sending email on behalf of a domain. DKIM allows receiving mail servers to check if the sending domain is authorized by verifying a DKIM key located in the domain’s DNS record against a DKIM signature located in the email.

**FREAK**: A SSL/TLS vulnerability that allows an attacker to intercept HTTPS connections between vulnerable clients and servers.

**POODLE**: A SSLv3 vulnerability that allows attackers to decrypt traffic to domains that support SSLv3

**Potentially Unwanted Applications (PUA)**: Infections such as grayware or adware; applications that may be installed on corporate devices without being vetted or without user knowledge.

**Shellshock**: a vulnerability that allows attackers to easily exploit non-Windows devices running unpatched versions of Bash.

**SPF (Sender Policy Framework)**: a DNS (Domain Name System) record that identifies which mail servers are permitted to send email on behalf of a domain. SPF records help prevent spammers from sending emails with forged From addresses.

---

2 To learn more about the FTC case against Wyndham: https://www.ftc.gov/news-events/press-releases/2012/06/ftc-files-complaint-against-wyndham-hotels-failure-protect