BITSIGHT *Insights*

BitSight Technologies Industry Report

Will Healthcare Be the Next Retail?

May 2014

BITSIGHT Insights

Will Healthcare Be The Next Retail?

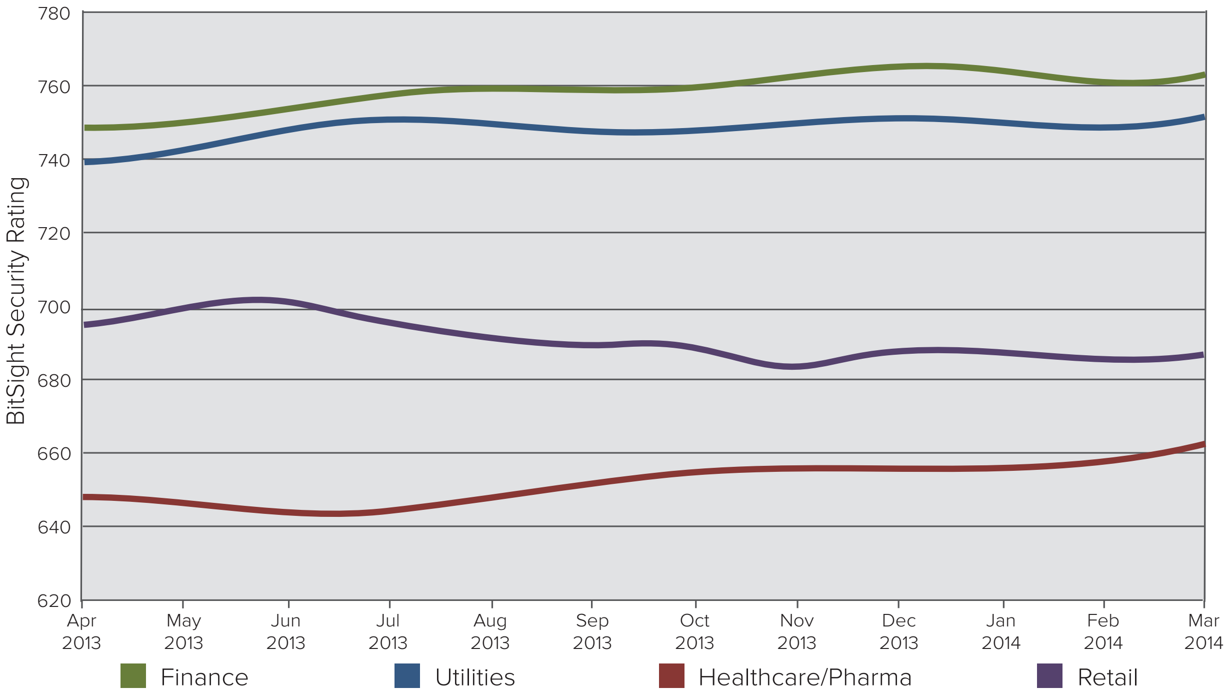
The news media has been ablaze with stories about cyber security in corporate America. Many of these stories talk about vulnerabilities in several sectors of the US economy, leaving us to question: which industries are the most secure?

BitSight Technologies uses external data to rate companies' security performance on a daily basis. Using vast amounts of data on observed security events, such as communication with a botnet, malware distribution or spam propagation, our daily Security Ratings provide a unique perspective on security risk, all from the outside. BitSight Security Ratings range from 250 to 900, with higher ratings equating to better security performance.

To assess the cyber health of the U.S. economy, BitSight analyzed the security performance of companies in the Standard & Poor's 500 stock index (S&P 500) in February 2014. We chose this index because of its broad representation of the American economy. Our analysis revealed that during 2013, 82% of these companies suffered from a security compromise.

Following on the heels of this analysis, we have examined the performance of four critical industries within the S&P 500: finance, utilities, retail, and healthcare and pharmaceuticals. Our analysis covers the time period from April 1, 2013 through March 31, 2014. Industry ratings are calculated using a simple average of the Security Ratings of companies in that sector.

BitSight Security Ratings by Industry



(Fig. 1) *Finance and Utilities lead the pack*

Key Findings

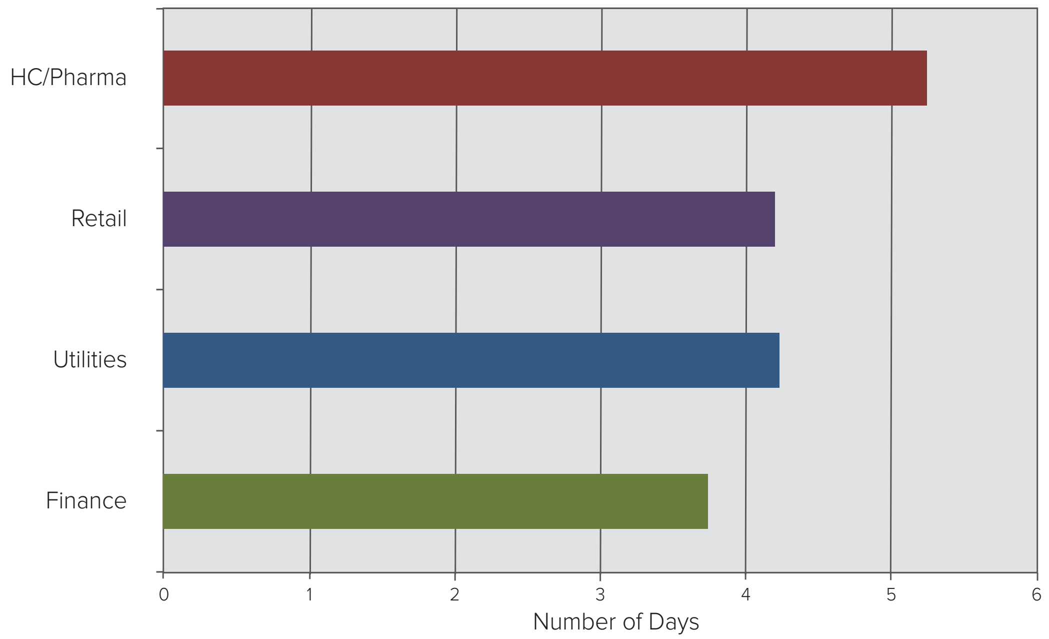
BitSight Technologies' latest analysis of Industry Security Ratings reveals significant differences among industries. Industry Security Ratings are based on companies in the S&P 500. Our key findings are below:

- The healthcare sector has many of the same characteristics as the retail sector, including a high volume of security incidents and slow response times. While its Security Rating has increased over the last few quarters, there is much room for improvement.

- The retail sector continues to be plagued with poor performance, with Security Ratings on the decline.

- Organizations that treat cyber security as a strategic issue perform better than those that view it as a tactical one. This helps to explain the superior Security Ratings of financial institutions and electric utilities in the S&P 500 compared to retailers and healthcare companies.

Average Event Duration by Industry



(Fig. 2) *Healthcare and Pharmaceuticals are slow to remediate security issues*

We use the following definitions in this report:

Security Event: External indicators of network compromise including spam propagation, malware observance, botnet infections, unsolicited communications and potentially exploited hosts.

Security Duration: The number of days between our first and last observance of a security event.

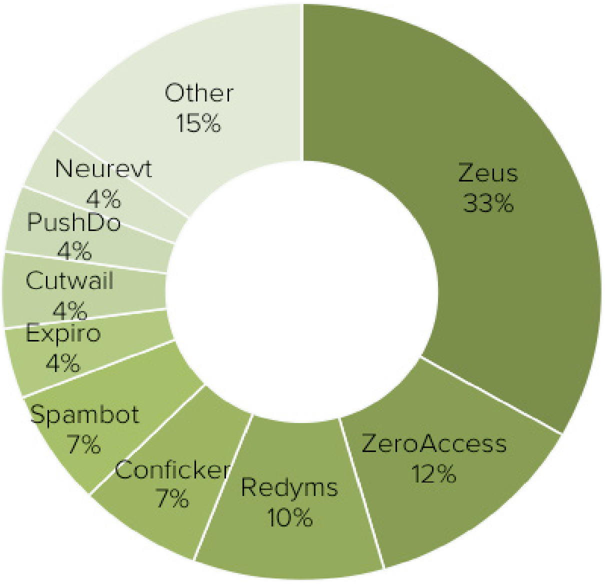
Finance | Utilities | Retail | Healthcare

Finance: Top of the Class

Key Findings

Finance is far and away the best industry performer in our analysis with a median industry Security Rating of 782.

- The finance Security Rating improved over the time period, ending Q1 2014 with an impressive average rating of 765.
- Zeus, a malware often used to steal banking information by man-in-the-browser keystroke logging, was the most prevalent malware observed by BitSight.
- Conficker, Redyms and Zero Access together made up approximately a third of the identified malware.



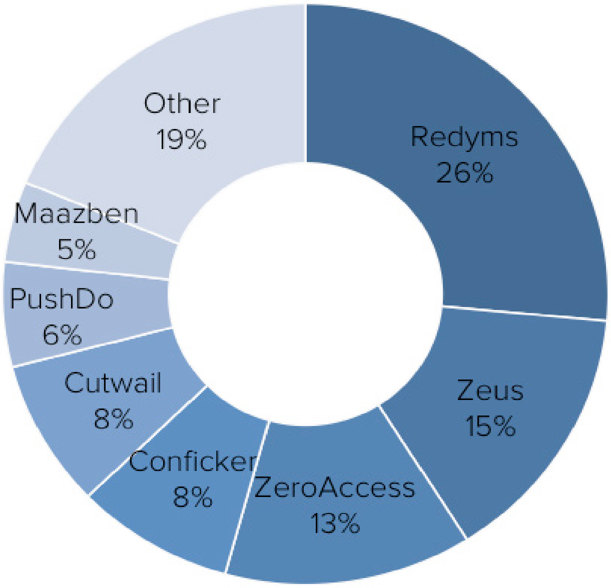
Observed Malware: Finance

Like all other industries included in our analysis, the number of security incidents in the networks of finance companies did increase over the time period. However, the finance sector had the shortest average event duration. (Fig. 2) This metric is an indication to the outside world of how quickly a company remediates issues. This suggests that this sector is quicker to detect and respond to cyber threats than other sectors.

So what other factors go into the high industry rating for finance? While our data speaks to security outcomes, there are clear indicators of why this industry is outperforming others. For one, these companies have a strong risk management culture. Like economic, financial, regulatory, and political risk, cyber security risk is also now part of ongoing business operations. In the PWC Global State of Information Security Survey 2014, 64% of respondents from North American financial institutions reported having a senior executive who proactively communicates the importance of information security to the entire organization, compared to 55% of respondents across all industry sectors in North America. In some cases, merely having a CISO or a comparable executive is not enough for financial institutions. BitSight's CTO, Stephen Boyer, recently attended the 2014 FS-ISAC & BITS Annual Summit and heard from risk management executives that companies are actively engaging with a potential business partner's CISO. "Effective risk management and detailed security plans are becoming selling points, making information security a competitive differentiator," says Boyer.

Moreover, financial institutions spend more on cyber security than their peers in other industries, and the largest ones tend to go well beyond the measures mandated by government and industry groups. Many of them share information on emerging industry level threats with their peers in the FS-Information Sharing and Analysis Center, an industry forum. In addition, regulations and guidelines from OCC (Office of the Comptroller of the Currency) and Federal Financial Institutions Examination Council (FFIEC) include comprehensive guidelines to mitigate network risk from external threats and third party networks.

Utilities: Shining Bright



Observed Malware: Utilities

Key Findings

Another strong performing group within the S&P 500 is the electric utilities.

- The sector saw an overall increase in their ratings, ending the year at 751.
- While the ratings of individual companies ranged from 590 to 820, the median rating over the time period was 760. Like finance, the range of ratings within the utilities sector is relatively narrow.
- Redyms, a family of trojans designed to redirect search engine results, hit this sector particularly hard. Zeus, Zero Access, Cutwail, and Conficker also infected machines in the utility sector.

Our findings may be surprising to many, particularly with all of the news about the need for better protection of our critical infrastructure against attacks from foreign hacker groups. The Department of Homeland Security recently reported responding to 198 cyber-incidents in 2012 across all critical sectors. Forty-one percent of these incidents involved the energy sector, particularly electricity.

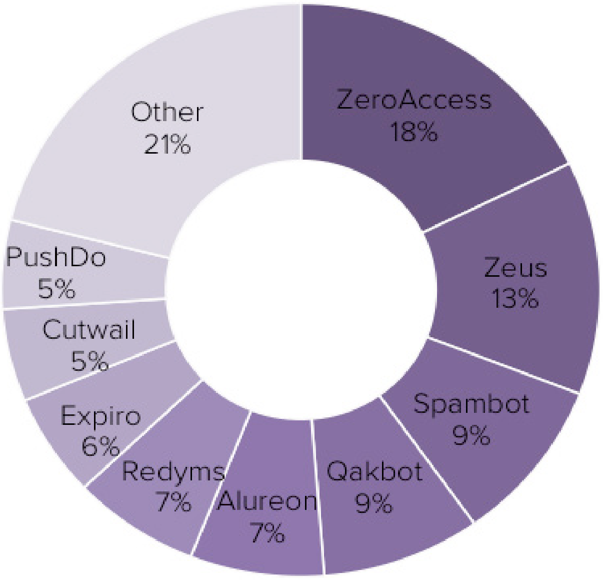
While the energy industry at large may be more vulnerable to cyber attacks, our analysis reveals that the nations largest utilities (those in the S&P 500) are actually quite good at protecting their public facing Internet assets[1]. Similar to finance, the generally positive security performance in this industry is likely the result of both executive level focus on cyber risk as well as industry regulation. The sector is highly regulated through the NERC CIP regulations, which have specific and prescriptive guidelines. The CIP Reliability Standards require 24 x 7 log monitoring and annual vulnerability tests. In addition, regulated entities must have an internal computer incident and response team to address any cyber security issues. All issues must be reported to the Electricity Sector Information Sharing and Analysis Center (ES ISAC). Version 5 of CIP Reliability Standards, approved in December 2013, extends the scope of the systems that are protected by the CIP Reliability Standards.

> ***"Large investor owned utilities have fairly sophisticated security practices. Like large financial institutions, they have significant security budgets and cyber risk has executive level visibility."***
>
> Dave Dalva, VP Security Science, Stroz Friedberg

The strong Security Ratings of the electric utilities in the S&P 500 are not surprising to some cyber security experts. Dave Dalva, VP of Security Science at Stroz Friedberg, notes, "In my experience, large investor owned utilities (IOUs) have fairly sophisticated IT security practices. Like large financial institutions, they have significant security budgets and cyber risk has executive level visibility." Dalva also believes that although NERC CIP only applies to portions of these IOUs (critical assets of the bulk electric system), it has led to a significant shift in attitudes towards cyber security in large utilities.

[1] BitSight's analysis is based only on evidence of compromise or vulnerability on externally facing IP networks.

Retail: Poor Performance Continues



Observed Malware: Retail

Key Findings

Within the past year, retail declined in security performance, ending the time period at an industry Security Rating of 685.

- The number of security events observed by BitSight increased nearly 200% from April 2013 to March 2014.
- Zeus, Zero Access, and Spambots were common malware found among the retailers of the S&P 500.
- Qakbot, a self propagating worm that was widespread in 2011, appears to be back. According to an Anubis Networks blog post in January 2014, the botnet owners control more than 20,000 infected PCs and are distributing new versions of the malware.

Retail has been center stage in the media coverage after last year's massive breaches that affected several major retailers such as Target, Neiman Marcus and Michaels. With mounting pressure to address this issue, retail executives have been bolstering cyber security programs by announcing new security-focused executives, revamping cyber defense initiatives and boosting IT security spending. And rightfully so. The recent data breaches have not only affected sales and stock prices, but also other measures such as consumer brand confidence. One recent survey published by Javelin Strategy and Research found 33% of consumers would avoid conducting business with a breached retailer. While a commitment to boosting cyber defenses is promising, the recent performance of the industry does not indicate improvement, but rather slow decline.

> "Cyber security still needs greater resources and executive level attention across the industry."
>
> Chris Poulin, IANS Faculty Member

While retailers scramble to assure others that they are taking meaningful steps to secure their networks, these numbers show little overall progress in the cyber health of the industry as a whole. It is important to note that this downward trend does not apply to all of the 31 retailers included in our analysis. Fourteen of the S&P retailers saw improvements in their Security Ratings. Of these improved performers, the median rise in ratings was a respectable 60 points. For the seventeen companies who saw an overall drop in their rating, the median drop was also 60 points. While a few are making modest gains in security performance, even more are steadily trending downward.

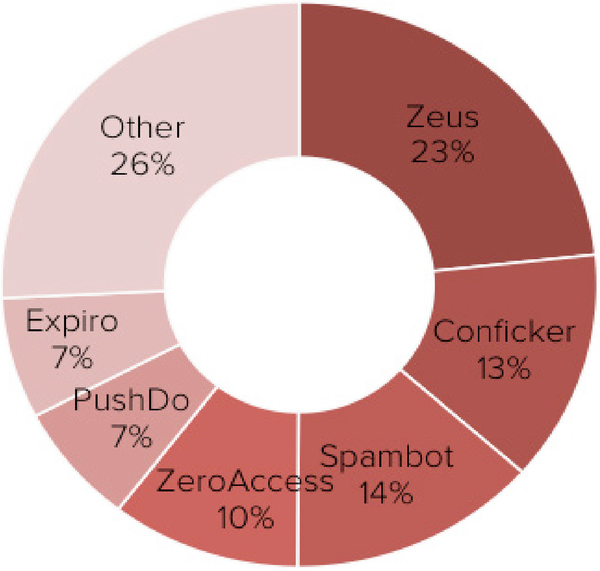
Chris Poulin, IANS Faculty Member, notes there is much retailers can learn from the risk management practices of leading financial institutions. "Some retailers do indeed have strong security practices, and the recent announcement from the Retail Industry Leaders Association (RILA) about the creation of a Retail Cyber Intelligence Sharing Center is certainly a step in the right direction. However, cyber security still needs greater resources and executive level attention across the industry."

Healthcare and Pharmaceuticals: The Next Retail?

Key Findings

Healthcare and pharmaceuticals saw an increase in security performance over the time period, ending Q1 2014 at approximately 660, close to retail.

- Security Ratings ranged from 410 to 820, with a median rating of 665. Like the retail sector, the spread in performance is large.
- This sector saw the largest percentage increase in the number of security incidents observed by BitSight over the time period.
- Average event duration is longer than any other industry, at a high of 5.3 days.



Observed Malware: HC/Pharma

Our findings echo the SANS 2014 Health Care Cyber Threat Report, which found “exploited medical devices, conferencing systems, web servers, printers and edge security technologies all sending out malicious traffic from medical organizations. Some of these devices and applications were openly exploitable (such as default admin passwords) for many months before the breached organization recognized or repaired the breach.” Our analysis confirms this finding, with the healthcare sector experiencing the longest average event duration of all industries we analyzed, at a worringly high 5.3 days.

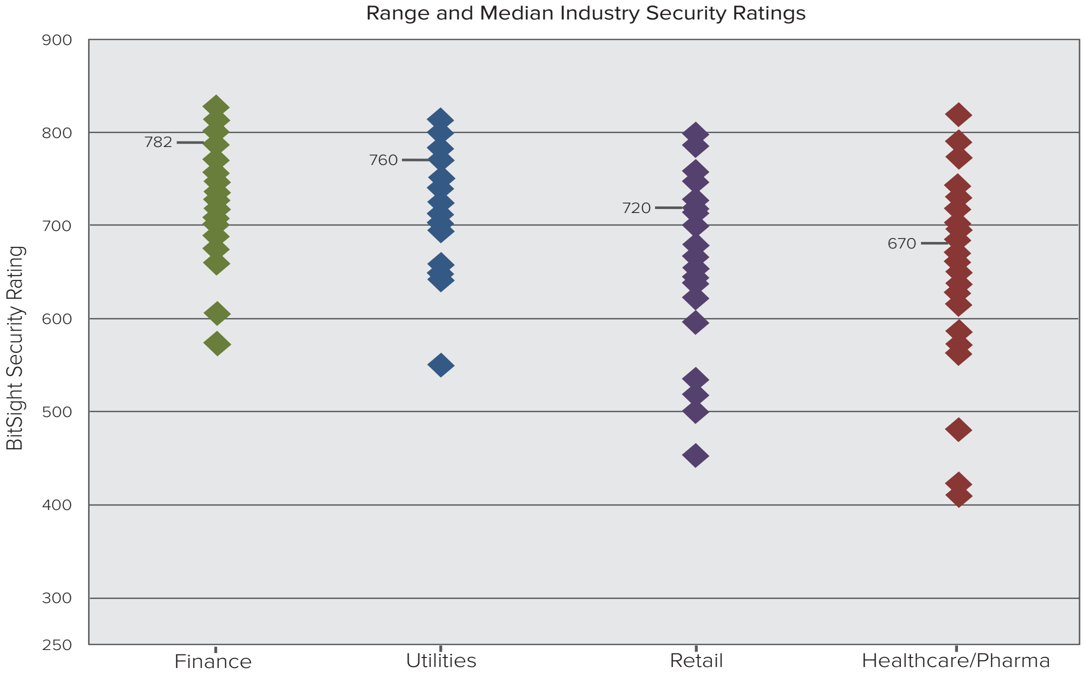
Chandu Ketkar, Technical Manager at Cigital, recently assessed medical devices used in clinics and hospitals around the country and discovered serious security concerns. “Weak encryption, lack of key management, poor authentication and authorization protocols, and insecure communications were all common findings that can compromise data confidentiality and integrity. When sensitive data is compromised, it can not only create risks for patients, but also expose health care providers and device manufacturers to regulatory and business risks.”

Unlike the financial institutions and electric utilities in the S&P 500, the healthcare and pharmaceutical companies do not view cyber security as a strategic business issue. They do not spend enough resources to protect their data, in part because cyber security has not received the executive level attention it deserves. According to a Ponemon study called “2013 Salary Benchmark Report,” the health and pharmaceutical sector ranks the lowest in compensation for information security staff. In general, this sector tends to spend only the resources required to be compliant with regulations such as HIPAA, and compliance does not equate to security. More prescriptive controls and better enforcement of HIPAA would certainly help improve security in the healthcare sector, along with a greater emphasis on security throughout these businesses.

This sector has also had a number of issues with theft and physical loss of laptops, servers and other devices that hold patient and personal data. In fact, Verizon’s 2014 Data Breach Incident Report found that theft and physical loss alone account for 46% of the industry’s breaches. Even more troubling, the 2014 Data Breach Industry Forecast states that “the healthcare industry, by far, will be the most susceptible to publicly disclosed and widely scrutinized data breaches in 2014,” a sentiment that BitSight certainly shares.

Conclusions

It is apparent from our analysis that not all companies within the S&P 500 are cut from the same cloth when it comes to cyber security performance. Some industries, notably finance and utilities, are taking the right steps to secure their networks. By no means are these sectors immune to growing and sophisticated attacks, but there is evidence that these industries have created a culture that raises cyber security issues to the highest level. The other two industries included in our analysis – retail and healthcare/pharma - have a much wider range of performance. While both include high performing companies, there are even more entities trending downward. Despite tougher regulations and increased public scrutiny, there remains substantial room for improvement.



(Fig. 3) *Industries with lower median ratings have a larger distribution of ratings*

In our last BitSight Insights, "Assessing the Cyber Health of the US Economy," we called the growing prominence of cyber security as an executive and board level issue, "good news." While that is undoubtedly still true, we also believe that companies need to enable better risk management through data. New initiatives and personnel are great first steps, but these people and programs need valuable metrics to continuously track performance. The availability of vast amounts of real time security data from both inside and outside of networks and access to better data processing tools can assist organizations in creating evidence-driven risk models. Companies can continuously evaluate and track security performance, enabling them to mitigate risks as they appear. By taking these next steps towards more responsible risk management, all industries of the US economy can see substantial and meaningful improvement in security performance.

BITSIGHT
THE STANDARD IN SECURITY RATINGS

About BitSight Technologies:
BitSight Technologies is transforming how companies manage information security risk with objective, evidence-based security ratings. The company's Security Rating Platform continuously analyzes vast amounts of external data on security behaviors in order to help organizations make timely risk management decisions.

125 Cambridge Park Drive, Cambridge, MA | www.bitsighttech.com | info@bitsighttech.com | 1.617.245.0469
Follow us on Twitter: @BitSight