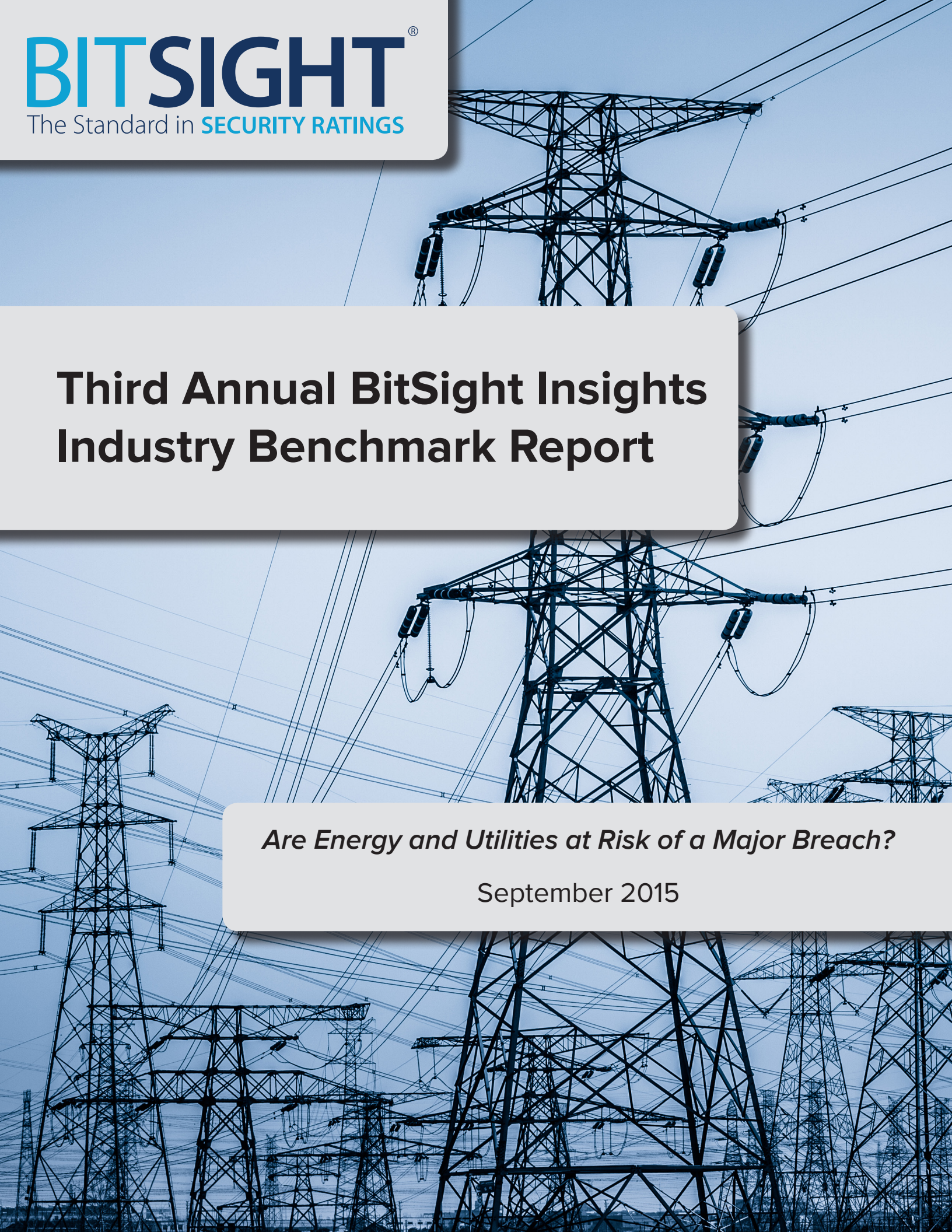
BITSIGHT®
The Standard in SECURITY RATINGS



Third Annual BitSight Insights Industry Benchmark Report

Are Energy and Utilities at Risk of a Major Breach?

September 2015

Introduction

Major breaches have affected companies and organizations across all sectors of the US economy from retail to healthcare, finance and government. As security leaders search for key performance indicators, industry metrics can serve as important benchmarks for understanding the performance of an organization and its portfolio of vendors.

Recognizing the growing importance of understanding cyber security posture, BitSight is publishing the Third Annual Industry Benchmarking Report. In this report, BitSight analyzed the security performance of six key industry sectors: Finance, Federal Government, Retail, Energy/Utilities, Healthcare and Education. These industries hold diverse types of data that are sensitive and valuable - especially to attackers. BitSight uses its proprietary Security Ratings algorithm, which takes into account diverse security metrics on events, diligence and user behaviors in order to derive aggregate industry metrics.

Risk management leaders and security practitioners can leverage the industry level data provided in this report for various initiatives including:

- Assessment of vendors in relation to industry averages
- Benchmarking an organization against industry averages and peers
- Cyber underwriting decision making
- Mergers and acquisitions due diligence
- Portfolio management

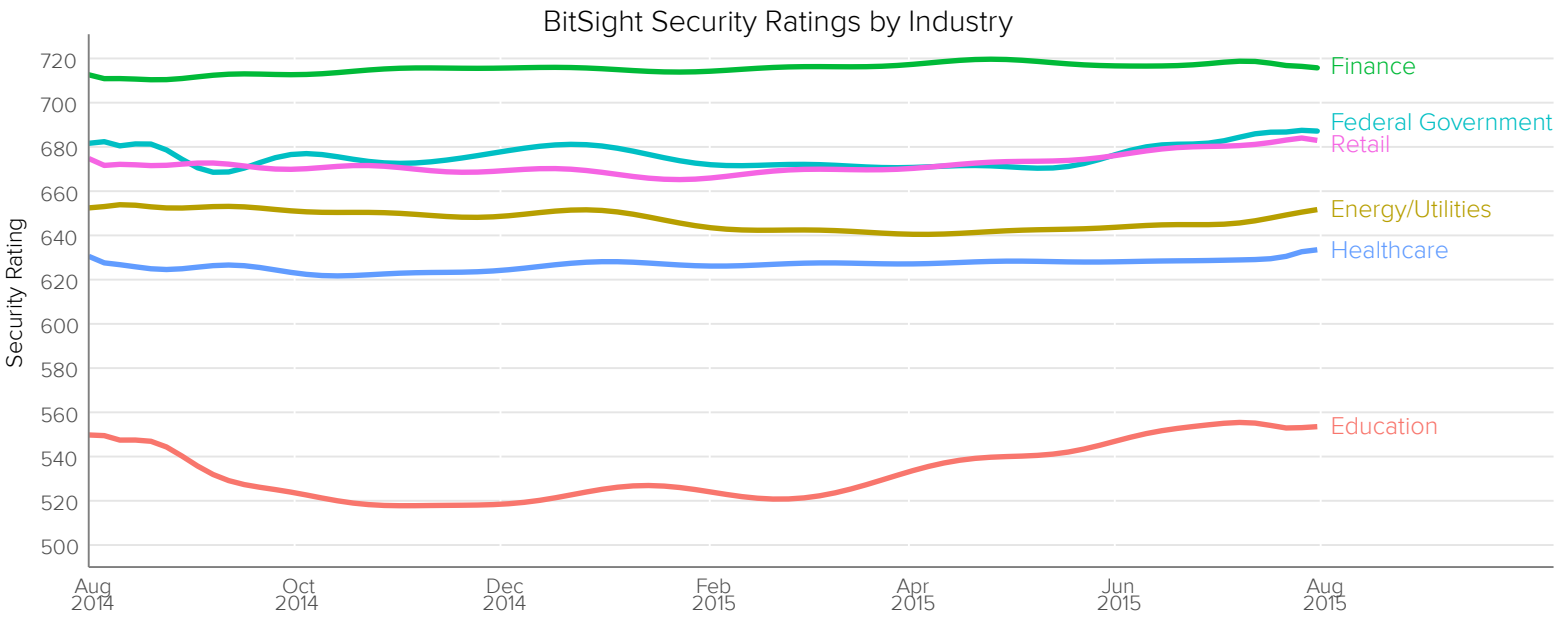


Figure 1

Key Findings

1. **Energy and Utilities are performing lower than the Retail sector and in-line with poorly performing Healthcare.**

   The Energy and Utilities industry is performing near the Healthcare industry when it comes to securing their networks against cyber attacks. In last year's industry report titled "Will Healthcare Be The Next Retail?" BitSight highlighted some troubling trends among healthcare companies such as an increase in the number of infections observed. Over the past year, BitSight researchers have noticed a dip in the performance of Energy and Utility companies from 653 to 652. As this industry connects previously isolated control systems to the internet it becomes increasingly important that a focus on operational technology (OT) does not overshadow the importance of information technology (IT) related threats such as a malware infection that could shut down the power grid.

2. **Companies across all industries are still vulnerable to major SSL vulnerabilities[1].**

   Companies in every industry sector are vulnerable to major SSL vulnerabilities such as Heartbleed, POODLE and FREAK. Given the widespread publicity surrounding some of these vulnerabilities, it is surprising that companies have servers running outdated and vulnerable versions of OpenSSL. While companies across all industries have mostly updated their servers to protect against Heartbleed, many companies have failed to act when it comes to POODLE and FREAK. For FREAK, industry vulnerability runs from 30% in Finance to 75% in Education. POODLE results are even more astounding: not one industry has more than 69% of companies protected. These SSL vulnerabilities can provide attackers with the ability to perform man in the middle attacks and extract sensitive information or gain private keys.

3. **The Federal Government - currently in the spotlight in the wake of the Office of Personnel Management mega breach - is the second highest performing sector, second only to Finance.**

   In July of this year, the New York Times broke news that a major cyber security breach had affected the Office of Personnel Management (OPM). The OPM breach, purportedly undertaken by Chinese hackers, compromised the records of 25.7 million records of current, former and prospective government employees and contractors[2]. Since this time, there have been consistent calls from lawmakers and Washington pundits for the government to get its cyber house in order. Nevertheless, our analysis of 119 different government entities shows that many of these agencies are performing well as a sector when it comes to overall security performance.

4. **Finance continues to be the top performing sector and Education the lowest.**

   Finance has consistently been the top performing industry in BitSight's industry benchmarking reports. BitSight attributes this consistent performance with a culture of awareness of cyber security issues, a mature regulatory landscape and adequate resources committed to protecting corporate networks. On the other end of the industry spectrum, educational institutions - and higher education in particular - are trailing other industries when it comes to protecting their networks. While educational institutions have unique network challenges to overcome, they are also becoming prime targets for the important intellectual property that they hold. This fact was recently highlighted by the recent intrusion of the University of Virginia's network by Chinese hackers[3].

SSL Vulnerabilities by Industry Sector

Heartbleed

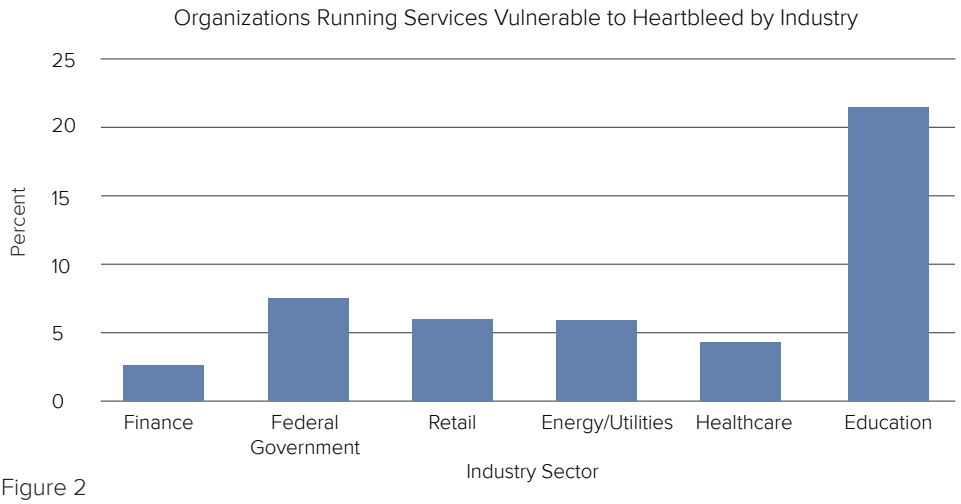


Figure 2

Industry	Percent
Finance	2.6%
Government	7.6%
Retail	5.6%
Energy/Utilities	5.2%
Healthcare	4.4%
Education	23.2%

FREAK

Industry	Percent
Finance	30.4%
Government	50.4%
Retail	37.1%
Energy/Utilities	40.5%
Healthcare	43.4%
Education	75.6%

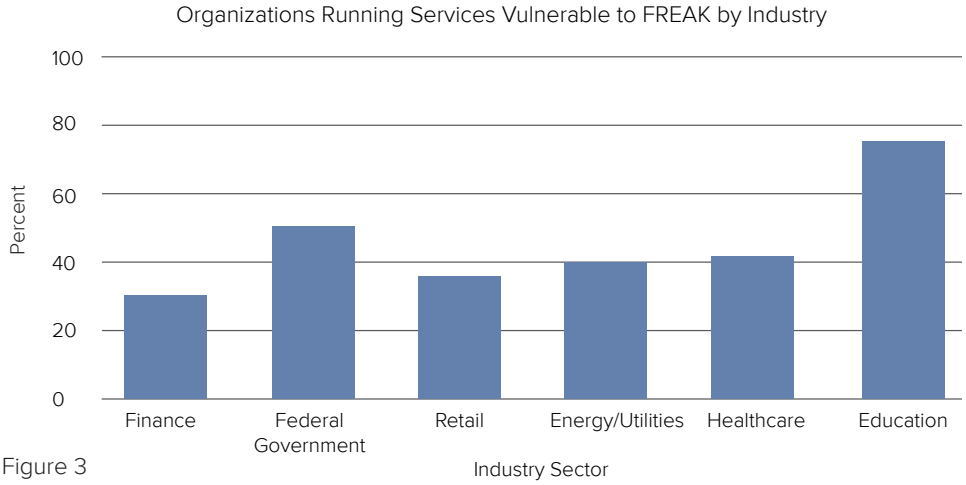


Figure 3

POODLE

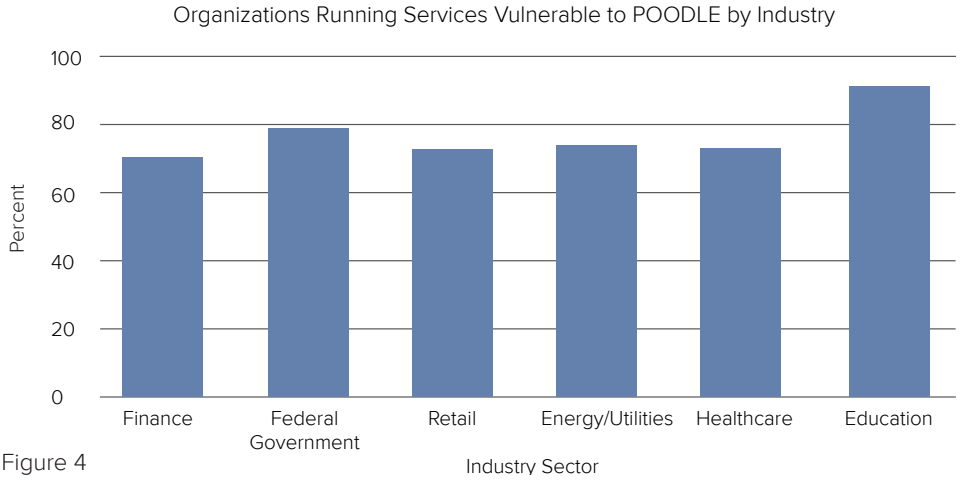


Figure 4

Industry	Percent
Finance	69%
Government	79%
Retail	72.2%
Energy/Utilities	74.8%
Healthcare	73.5%
Education	90.7%

Finance

Finance remains the top performing industry within our analysis. The industry's Security Rating was 716, which is inline with their rating of 712 a year earlier. When it comes to SSL vulnerabilities, this industry was also the top performer with only 2.6% vulnerable to Heartbleed. Nevertheless, 3 out of every 10 (30%) organizations were still vulnerable to FREAK and 7 out of 10 (69%) were vulnerable to POODLE. While this is better than other industry sectors, it still highlights an area for improvement for the industry.

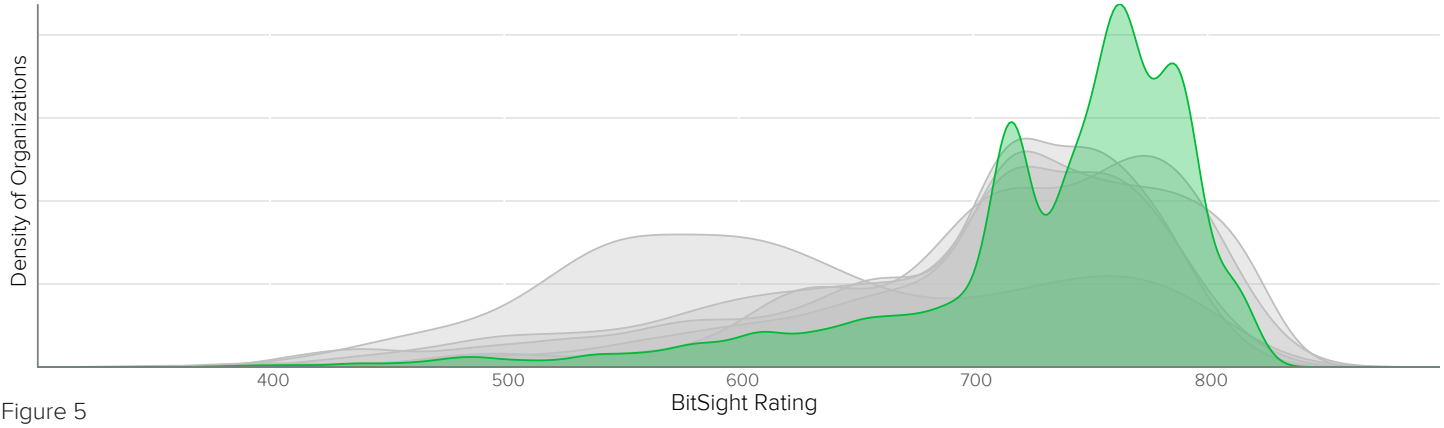


Figure 5

BitSight has consistently rated the Finance industry as a top performer. Financial institutions often make substantial investments to combat threats, with PwC noting that banks are planning on spending about $2 billion more in cyber security over the next two years[4]. In addition, banks and other financial institutions are faced with multiple regulations relating to cyber security promoting a risk aware culture. Another key to financial services success is a focus on mitigating threats posed by third party vendors. Financial services companies often have mature VRM programs that incorporate continuous monitoring of their vendor ecosystems and consistent audits of vendors[5]. In addition, organizations such as the Financial Services Information Sharing and Analysis Center (FS-ISAC), a key information exchange of threats to banks and financial services companies, have begun efforts to implement information exchanges in other industries that are critically important within the financial services vendor ecosystem. FS-ISAC has been instrumental in promoting information sharing through the establishment of a Legal ISAC[6] and a Retail ISAC[7].

Federal Government

While we have always tracked the security performance of government bodies, which include local, state, federal and international entities, we have not pulled out US federal government entities as a specific subsector. Thus, in light of the massive breach affecting the Office of Personnel Management, BitSight decided to include a category within this year's industry benchmarking report. This industry grouping consists of 119 federal government entities which focus on diverse disciplines, including healthcare, education, defense, diplomacy, budget, and more.

Since the OPM breach there have been loud cries from legislators, analysts and others that Washington needs to get its cyber defenses in order. A recent report by the Institute for Critical Infrastructure Technology noted that the this breach showed the "failings of the ill-equipped personnel, antiquated cyber security infrastructure, and abysmal security practices at the United States Office of Personnel Management." This report goes on to criticize a culture of awarding contracts to the lowest bidder for security work and a lack of vendor oversight - highlighted by the breaches of USIS and Keypoint, two government contractors with access to sensitive information[8].

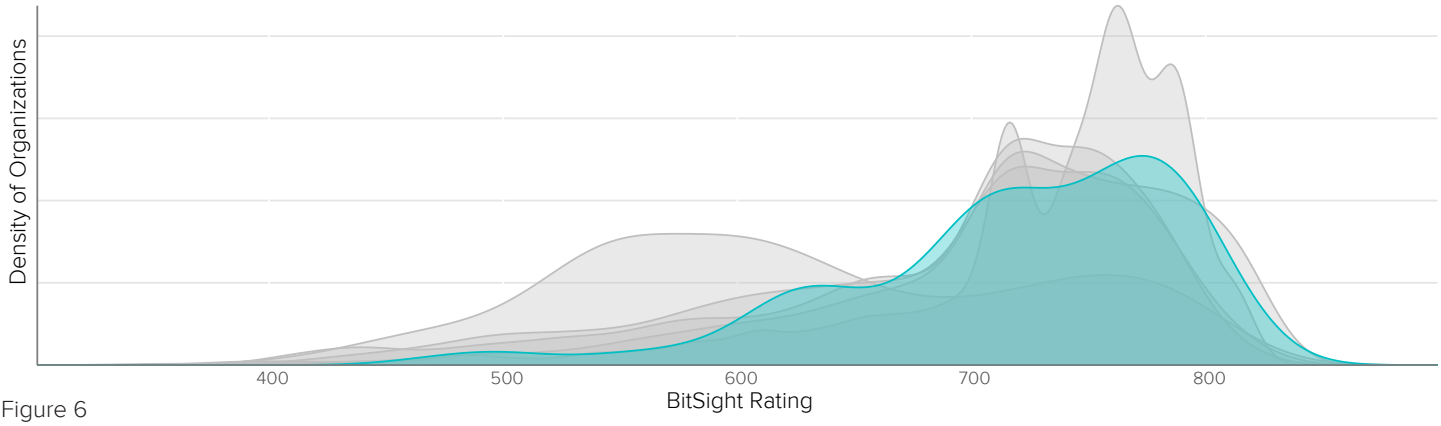


Figure 6

Although the OPM breach included massive data loss, BitSight data suggests that many agencies are performing well as a sector in defending, detecting and recovering from network threats. The industry's Security Rating is the second highest at 688. Last year the industry's rating was 684. One area of concern is that they are the second worst industry when it comes to protecting against major SSL vulnerabilities. BitSight analysis shows that many agencies were still vulnerable to Heartbleed (7.6%), Freak (50.4%) and Poodle (79%).

Retail

Many within the information security community dubbed 2014 the year of the retail breach. From Michaels to Neiman Marcus, major American retailers were affected by large scale data breaches affecting millions of customers[9]. Studies have indicated that major breaches in the industry have shifted consumer attitudes toward using cash over plastic[10]. This is not good for business: consumers tend to spend more money when using debit and credit cards[11]. In addition, loyalty programs and business branded credit cards are important sales channels for major retailers and provide important demographic information.

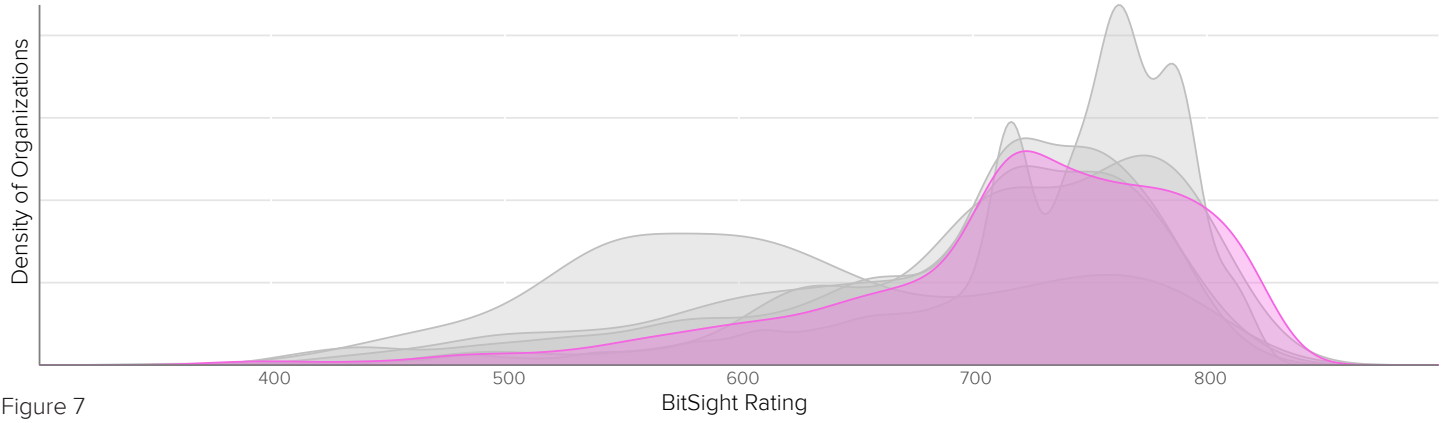


Figure 7

Responding to these challenges, 56% of retailers are actively investing more in their cyber security efforts according to BDO's Retail Compass Survey of CFOs[12]. There has also been an industry-wide push toward the adoption of EMV chip technology in store branded credit cards. Another positive improvement has been the inception of the R-ISC platform. This information sharing platform, supported by FS-ISAC, gives retailers access to information on emerging threats from peers, law enforcement and other reliable sources[13].

BitSight's analysis of the retail sector shows the industry's mean Security Rating was 684, putting it slightly below the federal government's rating. The sector saw slight improvement over the course of the year from last year's 674. Although, similar to all industries included in the report, the retail sector needs to ensure that it fully remediates SSL vulnerabilities. Currently, 5.6% of companies are vulnerable to Heartbleed, 37.1% are vulnerable to Freak and 72.2% are vulnerable to Poodle.

Energy and Utilities

There has been growing concern over the cyber security posture of Utility and Energy companies as more control systems are brought online. Various articles point to high stake losses related to a breach against Energy and Utility companies. Large insurer Lloyd's, in conjunction with researchers at the University of Cambridge, estimated potential losses from a cyber crime-induced blackout could hit $1 trillion[14]. The government has been diligently tracking attacks against the Energy industry. The government's Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) releases reports on cyber incidents affecting the country's critical infrastructure[15]. Interestingly, in 2014, the Energy sector was the most targeted sub-sector of the nation's critical infrastructure with 32% of incidents reported. The ICS-CERT Monitor also noted, "Of the total number of incidents reported to ICS-CERT, roughly 55 percent involved advanced persistent threats (APT) or sophisticated actors. Other actor types included hacktivists, insider threats, and criminals."

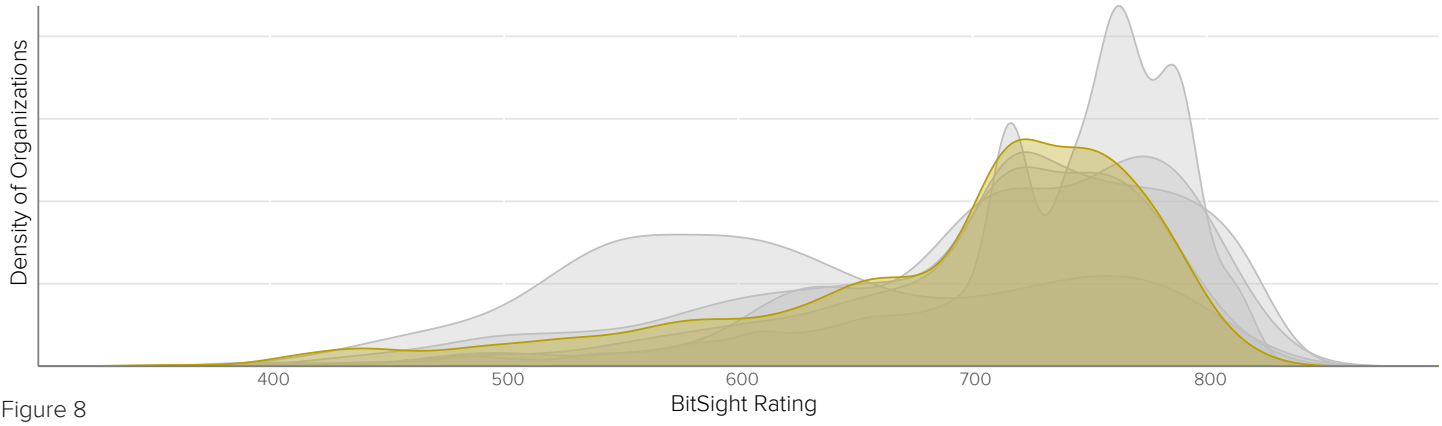


Figure 8

While many focus on worst-case scenarios, there are important challenges ahead for Energy and Utility companies. As operational technologies (systems that control the power grid, gas gauges, etc) become internet-enabled, these organizations must understand and anticipate information technology (IT) risks. The Congressional Research Service recently published a report that stated, "Modernization of many systems also has resulted in connections to the Internet. While these advances will improve the efficiency and performance of the grid, they will increase its vulnerability to potential cyberattacks"[16]. So what does this mean for Energy and Utility companies? SANS recently published a report on IT/OT convergence and explained: "For example, building automation systems, rife with networked monitoring, control and reporting devices can be interrupted either by attacking the devices individually or disrupting the network itself, and automated pharmaceutical production can be halted by events as simple to implement as buffer overflow or denial of service attacks"[17].

BitSight data provides empirical evidence to support the notion that there are challenges among Energy and Utility companies when it comes to securing their networks. The industry rating on August 1, 2015 was 652 which is relatively unchanged from last year's 653 but falls well below the retail sector. As we have noted within the other industry sectors, Energy and Utility companies need to shore up their servers to protect against SSL vulnerabilities. Companies in this sector are still vulnerable to Heartbleed (5.2%), Freak (40.5%) and Poodle (74.8%).

.

Healthcare

As highlighted in our previous BitSight Insights report, the healthcare sector continues to lag behind other sectors as the second worst industry performer. Within the past year, major breaches have affected healthcare providers and insurers both of which have access to sensitive personally identifiable information (PII). These records are incredibly valuable on the black market. A recent story from NPR found an undisclosed website where a “value pack” of 10 Medicare numbers was for sale. The price? “It costs 22 bitcoin — about $4,700 according to today’s exchange rate”[18].

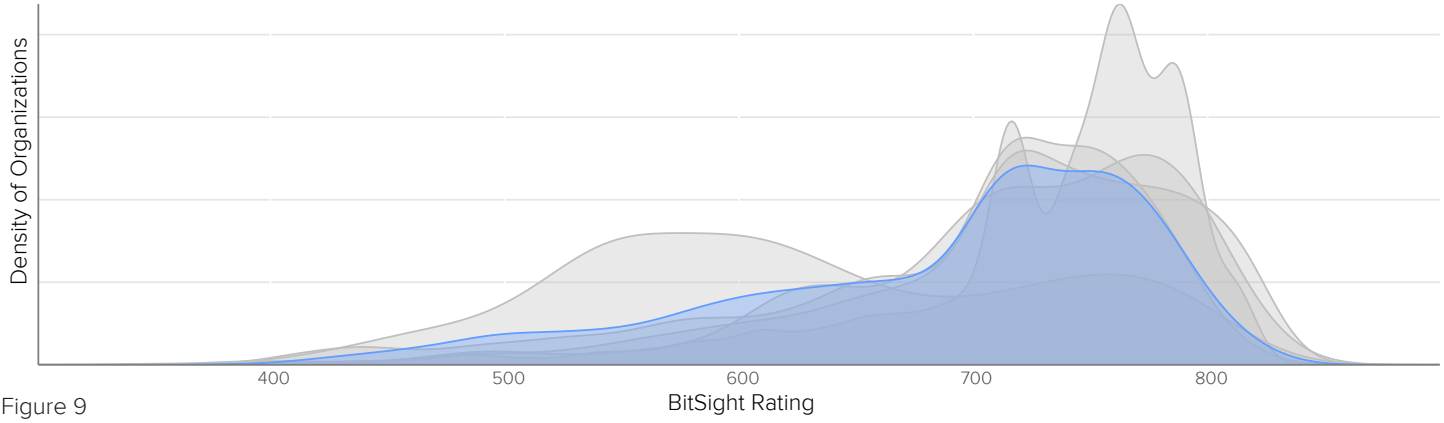


Figure 9

While HIPAA regulations attempt to ensure patient privacy and security of medical records, certain studies indicate a rise in incidents. A comprehensive study in the Journal of the American Medical Association analyzed the Department of Health and Human Services database on HIPAA disclosures of the loss of protected health information affecting at least 500 individuals from 2010-2013[19]. The study found that there were 949 data breaches during the time period, with 29 million records affected.

BitSight has continued to see stagnant performance across the industry as a whole. The Security Rating is practically unchanged at 634 (last year it was 630). The industry had the second lowest percentage of companies vulnerable to Heartbleed at 4.4%. Yet a high percentage of companies remain vulnerable to Freak (43.4%) and Poodle (73.5%).

Education

BitSight continues to see Education as the lowest performing industry sector. This continued lag in performance echoes the sentiments of a previous BitSight Insights report that focused on the security posture of college athletic conferences[20]. BitSight found that colleges and universities have challenging network requirements, such as BYOD networks and multiple access points. Interestingly, that report found that universities that made proactive strategic investments in cyber security - such as hiring a dedicated CISO - far outperformed the industry average.

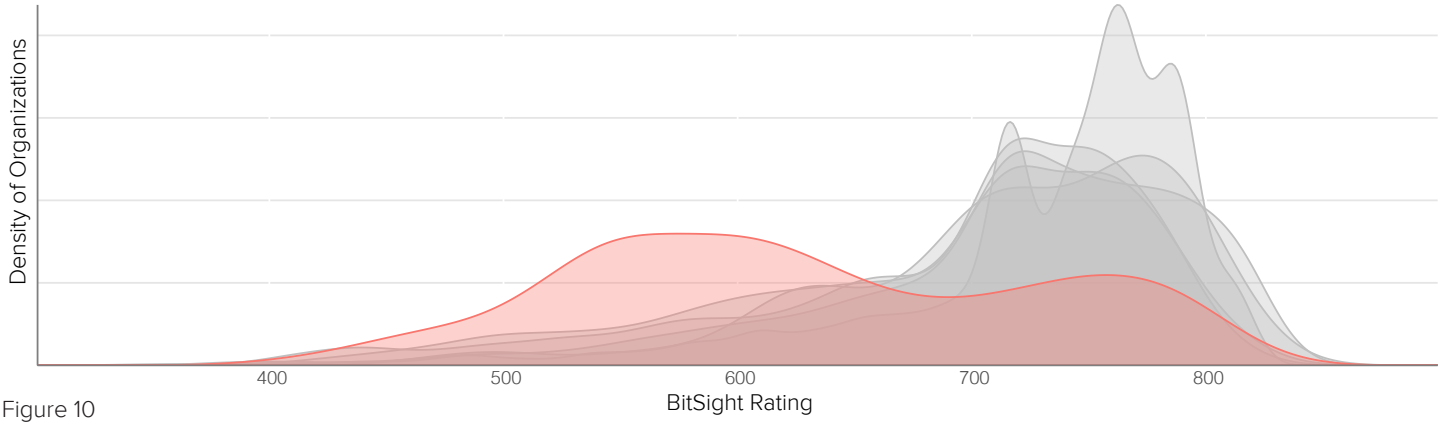


Figure 10

While universities continue to have unique network requirements and specific challenges to securing their networks, it is important to recognize the high-value information that these institutions hold. America's colleges and universities produce cutting edge research in technology and the sciences that can be leveraged for commercial gain. Within the past year there have been targeted attacks, some of which have been attributed to Chinese hackers, against major research universities such as the University of Connecticut[21] and Penn State[22].

The industry's rating as of August 1 was a low 554, compared to 551 as of last year. This is the second year in a row that we have observed a drop in the industry's rating during the months of the school year. While we cannot definitively say why there is a drop during these months, it is likely that as more students and devices enter a university or school's network BitSight observes more infections emanating from that network. When it comes to the remediation of SSL vulnerabilities, the Education sector is also the lowest performing industry with a large percentage of organizations still vulnerable to Heartbleed (23.2%), Freak (75.9%) and Poodle (90.7%).

Conclusion

As businesses invest more time and resources into addressing cyber security concerns, the findings of this report are relevant to the decision making processes. For security practitioners, these metrics can inform security benchmarking initiatives that answer a crucial question: How are we doing compared to industry peers? In addition, vendor risk teams and cyber insurance underwriters can look at third parties or applicants in relation to industry performance metrics. This insight can inform whether a company is willing to share sensitive data with a third party vendor or affect how a cyber insurance underwriter prices the risk of an insurance applicant. Businesses involved in mergers and acquisitions or portfolio management can look at potential and current investments to gauge whether to invest in a company or whether to set performance guidelines.

As cyber security enters the boardroom, industry level benchmarks serve as a key talking point and performance indicator for many businesses. Using this data in conjunction with continuous ratings and metrics on the health of a company's security posture --and the posture of its vendors-- allows organizations to build a risk aware security program that mitigates threats as they appear.

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 | info@bitsighttech.com

Study Overview and Methodology

To perform this industry analysis, BitSight sampled the daily mean Security Ratings for each of six industry sectors from August 1, 2014 to August 1, 2015, which includes 9, 708 companies. BitSight also extracted industry level data on specific security metrics that are factored into the rating, such as distribution of ratings and SSL vulnerability data related to Heartbleed, POODLE and FREAK.

BitSight Security Ratings range between 250 and 900, with higher ratings indicating better performance. These ratings are calculated using terabytes of data, including nearly 4 years of historical information, on risk vectors 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.

BITSIGHT®
The Standard in SECURITY RATINGS

References and Citations

1. 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

2. Information about OPM Cybersecurity Incidents. (n.d.) https://www.opm.gov/cybersecurity. Retrieved August 1, 2015.

3. Bo Williams, K. (2015, August 21) University of Virginia hack targeted employees with China ties. *The Hill*. Retrieved from: http://thehill.com/policy/cybersecurity/251643-uva-hack-targeted-individuals-with-china-ties

4. Huang, D., Glazer, E., & Yadron, D. (2015, November 17). Financial Firms Bolster Cybersecurity Budgets. *Wall Street Journal*. Retrieved September 1, 2015, from http://www.wsj.com/articles/financial-firms-bolster-cybersecurity-budgets-1416182536

5. Learn more on the BitSight blog: http://blog.bitsighttech.com/managing-vendor-risk-complexity-financial-institution

6. Simmons, C., & Gluckman, N. (2015, March 4). Law Firms to Form Cybersecurity Alliance. *The American Lawyer.* Retrieved September 20, 2015, from
http://www.americanlawyer.com/id=1202719660496/Law-Firms-to-Form-Cybersecurity-Alliance?slreturn=20150820164629

7. Retail-ISAC launches Cyber Sharing Portal Supported by FS-ISAC. (2015, March 24). *PR Newswire*. Retrieved from http://www.prnewswire.com/news-releases/retail-isac-launches-cyber-sharing-portal-supported-by-fs-isac-300055086.html

8. Handing Over the Keys to the Castle: OPM Demonstrated that Antiquated Security Practices Harm National Security. (2015, July 1). *Institute for Critical Infrastructure Technology*.

9. Jackson Higgins, K. (2014, November 11). The Year of the Retailer Data Breach. *Dark Reading*.
http://www.darkreading.com/attacks-breaches/the-year-of-the-retailer-data-breach/d/d-id/1317462

10. Wilson, T. (2014, July 7). Retail Breaches Change Customer Behavior, Attitudes, Studies Say. *Dark Reading*.
http://www.darkreading.com/retail-breaches-change-customer-behavior-attitudes-studies-say/d/d-id/1279144

11. Konsko, L. (2014, July 8). Credit Cards Make You Spend More: Study. *Nerdwallet*.
http://www.nerdwallet.com/blog/credit-cards/credit-cards-make-you-spend-more/

12. Retailers Offer Bright 2015 Outlook Rife with M&A Activity (2015 April) *BDO Website*. Retrieved from:
https://www.bdo.com/insights/industries/retail-consumer-products/2015-retail-compass-survey-of-cfos

13. For more information of R-CISC: https://r-cisc.org

14. Bergen, M. (2015, July 8). Cost of a Potential Blackout From Cyber Crime: $1 Trillion. *Re/code*.
http://recode.net/2015/07/08/cost-of-a-potential-blackout-from-cyber-crime-1-trillion/

15. ICS-CERT Monitor (September 2014 - February 2015) Retrieved from (PDF):
https://ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_Sep2014-Feb2015.pdf

16. Campbell, R. (2014 June 10) Cybersecurity Issues for the Bulk Power System. *Congressional Research Service.* Retrieved from: https://www.fas.org/sgp/crs/misc/R43989.pdf (PDF)

17. Harp, D. & Gregory-Brown, B. (n.d.) IT/OT Convergence: Bridging the Divide. *SANS*. Retrieved from:
http://ics.sans.org/media/IT-OT-Convergence-NexDefense-Whitepaper.pdf

18. Shahani, A. (2015 February 13) The Black Market For Stolen Health Care Data. *NPR All Things Considered*. Retrieved from:
http://www.npr.org/sections/alltechconsidered/2015/02/13/385901377/the-black-market-for-stolen-health-care-data

19. Liu V, Musen M. & Chou T. (2015 April 14) Data Breaches of Protected Health Information in the United States. Retrieved from (paywall): http://jama.jamanetwork.com/article.aspx?articleid=2247135

20. BitSight published a comprehensive education benchmarking report in August 2014. Learn more here:
http://blog.bisighttech.com/bitsight-insights-powerhouses-and-benchwarmers

21. Weizel, R. (2015 July 31) University of Connecticut says hit by hackers from China. *Reuters*. Retrieved from:
http://www.reuters.com/article/2015/07/31/us-usa-connecticut-cyberattack-idUSKCN0Q52I320150731

22. Hesseldahl, A. (2015 May 15) Penn State Engineering School Cuts Off Internet After Hacking Attacks. *Re/code*. Retrieved from: http://recode.net/2015/05/15/penn-state-engineering-school-cuts-off-internet-after-hacking-attacks/