Consumer Protection and Cybersecurity: The Consumer Education Gap

By: David Serabian

Executive Summary

Consumer cyber protection as it relates to the threat of cyber insecurity is an increasingly critical issue with cyberattacks on major businesses such as Target and Sony. Over 100 million Americans to date have had their financial information compromised, and in the ten-year history of Verizon's Payment Card Industry investigations no companies were compliant with Payment Card Industry standards at the time of the attack. In March 2015, the FCC fined AT&T $25 million for failing to adequately provide cybersecurity that resulted in almost 300,000 people having their personal and financial information compromised. It was the largest in FCC history of this type.

According to Fujitsu, consumer trust has reached a 10-year low, and only nine percent consumers say they believe a company will adequately secure their data. A report in April 2014 by Radius Global Market Research indicated that consumers are more concerned about online security, online privacy, identity theft, and fraud than other social issues such as unemployment, obesity, health insurance, and gun control. Consumers do not have a means to know how good the cybersecurity is of companies that they give their financial information to. As a result, an asymmetric information problem is taking place and the result is inefficiency in the market.

The President announced in January 2015 that cybersecurity for consumers is important enough to warrant new legislation. The Federal Trade Commission has established a new office dedicated to researching and educating consumers about the risks of new technologies. These indicate a clear shift in policy by the government to cybersecurity and consumer protection.

The Consumer Financial Protection Bureau (CFPB) should take its mandate to educate and create a letter grade rating system to rate companies on their cybersecurity to support the Executive branch mission to help protect consumers as announced by the President. This report card on companies would educate and allow consumers to better decide which companies to trust with their financial future and information. This system can be based off the 12 factors in the already existing Payment Card Industry guidelines. With this information consumers would be better able to decide what companies to use, and encourage companies through consumer choice to improve the cybersecurity of their customers' information.

Facts

- 100 million Americans have had their financial information compromised so far
- In 10 years no company investigated by Verizon's Payment Card Industry Investigation Report has been compliant with industry cybersecurity standards
- Only 9% of consumers feel that companies will adequately secure their data
- In April 2015 the FCC fined AT&T $25 million dollars for failing to adequately secure consumer information in the largest penalty over cybersecurity to date
- Consumers are more concerned with online security, online privacy, identity theft, and fraud than other issues like unemployment, obesity, health insurance, and gun control
- Consumers do not know the quality of cybersecurity that a company provides
- The Consumer Financial Protection Bureau has a mandate to educate and protect consumers

Recommendations

- The CFPB should create a letter grade rating system based upon Payment Card Industry Guidelines
- This report card would allow consumers to make better decisions on which companies they will trust with their financial information
- This report card would also encourage companies to improve their cybersecurity in order to be competitive in the market as consumers choose companies with better cybersecurity

Introduction

Cyber protection as it relates to the threat of cyber insecurity is an increasingly critical issue with over 100 million Americans to date having their financial information compromised. Consumers are willing to pay more for companies that secure their information, and their concern for protection of their financial information is greater than their concern for issues like healthcare and gun control.[1] The President has announced legislation to protect consumers' financial information online, and along with the President's announcement, the Federal Communications Commission (FCC) has begun to crack down on companies with inadequate and compromised consumer information. However, educating consumers is necessary because of a cybersecurity consumer education gap that is occurring where consumers do not know the cybersecurity risks of companies they are trusting with their financial information.

When consumers are informed of the potential cybersecurity risk it helps them in two ways. First, it gives consumers information that they can use in choosing the businesses with better security; and second, by educating consumers, it can help increase market demand for increased cybersecurity. So far consumer education by the Federal government is lacking as this is a new field of policy. The Consumer Financial Protection Bureau (CFPB) has a mandate to educate consumers about financial risks, especially following the 2008 global financial meltdown that was the driving force behind its creation. The CFPB should take its mandate to educate and inform consumers of the cyber protection that companies have for consumer information using industry standards just as Medicare has done with rating hospitals and help close the cybersecurity consumer education gap.

The Problem

Cybersecurity and consumer protection continue to be a growing issue as well as one for concern. From cyberattacks that shut down online services for video game consoles,[2] to the Islamic State defacing the Twitter account of U.S. Central Command in April 2014.[3] Frequent news of some type of cyberattack is becoming the norm in today's society. The responses to these attacks have varied from FBI investigations[4] and arrests of hackers[5] [6] to lawsuits brought by consumers' information on companies that did not secure their information as what happened to Target.[7] In the case of Target, those lawsuits were settled out of court for millions of dollars.[8]

> Verizon for the last ten years has investigated PCI payment breaches and in those ten years none, absolutely *none*, of the organizations were compliant with PCI DSS at the time of the breach

The guidelines for cybersecurity that have been created by the Payment Card Industry have not been fully put into place, especially in the case of the Payment Card Industry Data Security Standard (PCI DSS). PCI data security standards were established in 2004 and have been periodically updated with the current guidelines having 12 requirements.[9] Verizon for the last ten years has investigated PCI payment breaches and in those ten years none, absolutely *none*, of the organizations were compliant with PCI DSS at the time of the breach as of the 2015 report.[10] Despite the recent high profile cases of cyberattacks and data breaches with payment cards, many companies still are not compliant and view the guidelines more as a checklist that is looked at once a year rather than a standard to aspire to. Even with the once a year, checklist only 20% of

organizations passed the initial 2014 PCI compliance assessment.[11]

The Federal Communications Commission (FCC) has tasked itself with protecting consumers' financial information from unauthorized use even if the information itself was not necessarily exploited due to a lack of security. In October 2014, the FCC imposed a fine of $10 million on TerraCom and YourTel for failing to protect consumers' personal information (PI).[12] The FCC stated that these companies had violated sections of the Communications Act of 1934 because they misled their customers by stating in the privacy policies that they used sufficient technology to protect the data of their customers. They were not employing even a reasonable amount of security for consumer information, and did not inform customers if their information had been compromised.[13] This fine was particularly important because these telecommunication companies provide services for the Lifeline program, which provides discounted phone service for eligible low-income persons in order to allow them to get a job, contact emergency services, and connect with family.[14]

The Lifeline program required consumers to submit financial information indicating that they had low income by showing they made below the federally defined poverty line, or participated in government assistance programs such as discounted/free school lunch, food stamps, etc. Providing this information required providing more than just credit card information, but also a Social Security number, driver's license, date of birth, and the like to provide proof of eligibility. Customers were required to scan and upload this information to the companies in order to determine if they qualified.[15] The companies' data security was so minimal that an unauthorized person could use an internet search engine, and (with some manipulation) be able to access the PI of these customers.[16]

However, the lack of protection of data as in the case of the TerraCom and YourTel is not the only reason for data breaches. In April 2015 the FCC entered a $25 million settlement with AT&T over data breaches that resulted in almost 300,000 customers' privacy information including Social Security numbers being disclosed.[17] Call centers that AT&T used in countries like Colombia, the Philippines, and Mexico inappropriately accessed consumers information, and used that data to sell to others who trafficked in stolen cell phones and needed the unlock codes.

In the case of AT&T it was people who had access to the information within the country that disclosed the information, and could have been avoided if AT&T had exercised better decision-making. The human factor unfortunately is something that will also be with us, and is a deciding factor in these data breaches. It is not simply a matter of trusting people within your organization anymore as seen with AT&T, but also keeping a watchful eye on your personnel within your organization as part of a company's cybersecurity. One of the biggest risks to a company's data security is an employee,[18] and employees maintaining password word security is vital to ensuring consumer safety. Through poor training, not enough background checks on employees, bad management, or whatever the case may be AT&T ultimately made poor decisions. This was also the case with Target where adequate warning of a compromise was received, but no action was taken to prevent it.[19] Unfortunately, no matter how smart that you are quite often in the case of cyberattacks smart people are making poor decisions, and something needs to be done.[20]

Why Something Needs to be Done

In economic terms there is an asymmetric information problem taking place that is resulting in an inefficient market. The consumer does not know the quality of the cybersecurity that will be provided for their financial information, but the company providing the protection does. If a financial company has good interest rates for the consumer, then the customer will find that more attractive. However, if that consumer also finds out that the company has poor cybersecurity and thereby a cyber-breach could negatively affect

their credit, the consumer would rationally take that into account into their decision making process. However, due to the cybersecurity consumer education gap there is no quality-checking middleman to inform consumers of the risks of companies with weak cybersecurity. Companies have credit ratings, consumers have credit ratings, but the cybersecurity of companies do not have ratings. There is no "Better Business Bureau" of consumer information rated to cybersecurity, and thus consumers are blind to the risks.

> "There is no 'Better Business Bureau' of consumer information rated to cybersecurity"

Cyber security is of great importance especially for financial institutions as they become increasingly more connected,[21] and as new types of crimes develop when a new technology emerges (mail fraud, wire fraud, phone fraud, etc.). Cybercrime "looks to be a permanent feature of the online ecosystem"[22] and thus must be dealt with. The economic damage is significant as companies lose money due to data breaches in the stock market,[23] and in one study companies on average lost approximately 6% in stock value[24]. Organizations also have to deal with an average cost of $5.4 million for a data breach in the U.S., higher than anywhere else in the world.[25]

This also creates distortionary behavior in consumers who will change what they do online from higher value activities to lower value activities in order to reduce the risk of their information from being compromised.[26] Perhaps one of the best quotes on this issue comes from a report on the risks of a hyper connected world by McKinsey and Company "the global economy is still not sufficiently protected against cyberattacks—and it is getting worse."[27] Yet despite all the harm that can occur to a company's bottom line companies still are not adequately protecting themselves, and trust in companies is degrading as a result.

Trust is needed for society and markets as part of society to operate,[28] and cyberattacks act as a way to degrade the trust in society.[29] According to a December 2013 report by Fujitsu consumer trust has reached a 10-year low, with only nine percent of consumers having faith that brands will be able to keep their data secure.[30] Without confidence in businesses because they have weak cybersecurity, consumers will be less likely to spend, and ultimately results in these cyberattacks weakening the economy as hole.

Consumers have recognized that cybersecurity is important with online security being a more important social issue to consumers than health insurance, obesity, and gun control according to an April 2014 study by Radius Global Market Research.[31] Polled consumers stated that the top four important social issues were online security (87%), online privacy (85%), identity theft (83%), and fraud (79%).[32] Despite the 2008 financial crisis still fresh in peoples' minds, unemployment as a social issue was rated by consumers as being less important than those four issues, and over half of those surveyed had an experience with identity theft.[33]

More telling was that of all the industries that could be rated as keeping consumers' information safe, the option for "no industry" received the highest ranking. In almost every industry, "consumers feel that the responsibility for online security falls squarely on the company. The single exception is with social media sites like Facebook, Twitter and Instagram where more consumers feel it is their own responsibility to keep information secure."[34] As attention is given to the Affordable Care Act, the increasing health issues with obesity, and active shooter attacks, the public is more concerned with online security than any of these issues. Despite the attention that these other issues have received the government should act and address citizens' concerns.

Benefits of Government Action

Consumers have a right to understand the risks that they face when using their credit and debit cards for transaction, whether they be in person or online. The CFPB as one of its mandates

is to educate consumers on financial issues.[35] On their website there are insightful videos and other information on how to protect oneself from having their financial information stolen. As well as how to respond if information has been compromised or is being exploited; especially when loans and credit cards are taken out in the name of the victim without their knowledge as a result of identity theft. This is an attempt to proactively inform consumers and address how to act before and after financial information is compromised, instead of a company informing consumers what could have been done after loans have been taken out in their name. With the CFPB informing consumers instead of a company the consumers benefit, because the goal of the CFPB is to help protect consumers whereas a company is focused on protecting its own interests and not necessarily consumers.

With government action taking place to correct this market inefficiency, consumers would be able to have a better chance of preventing their financial information from being compromised because the government's goals would be more aligned with consumers. With this information in consumer hands the market would be more likely to correct itself. According to that same Radius Global Marketing Research poll consumers have stated that 50% of consumers would be willing to pay more for a company that values their privacy more, and 69% of consumers stating they would be less inclined to buy from a company that has had a security breach.[36]

If a company can offer a special cybersecurity service, perhaps some kind of financial guarantee, that will not only increase the trust of the customer in the product but will also give a company a competitive edge over their competition for consumers. Undoubtedly some companies will win and some will lose, but those that can adapt and take ardent strides to improving their security will no doubt keep or gain customers. By educating consumers the government is not *hurting* the market but *helping* it by letting companies know how good or bad their competition is in an area of concern for consumers.

Educating consumers directly could be enacted more quickly than mandating specific security standards for companies through regulation or legislation. Even if the regulation or legislation stated that specifics had to be met, technology is changing and it can be difficult for regulation and legislation to keep up. A government agency can release an update (such as a press release or updated rating) about a company, and consumers can respond to that update faster than it would take for a regulation or law to be enacted. This would in no way act in place of legislation or regulation, but would complement them. Recently the government has taken steps to educate consumers and enforce cybersecurity standards through regulation

What Has Been Done

Educating consumers has been taken on as a new mantle of government responsibility. The CFPB was established after the 2008 financial crisis, and since then government agencies have been mandated (like the CFPB) or taken it upon themselves to protect and educate consumers, but this idea goes back far beyond that.

The protection of consumers for the sake of public welfare has been part of the government's responsibility since at least the establishment of the Food and Drug Administration.[37] Protecting consumers from the health risks of bad food and medicine has without a doubt been a great benefit to society that the government has been able to provide. At the local level consumers trust in government regulation through local health departments to regulate and assess the quality of food that consumer eat at restaurants. This is most often seen with some type of grade or rating given to a restaurant that must be prominently displayed so that consumers can know the health quality of the restaurant. The grading system itself educates consumers at the place of purchase concerning the quality of the restaurant.

With regard to informing consumers the government took a further step in April 2015, when the Centers for Medicare and Medicaid Services created both a database and a search engine on their website that allows consumers to search for hospitals and compare the rating of one hospital to others through a one to five star rating system.[38] This was created to better inform consumers about the practices and quality of care that they would be able to receive. The data that is used comes from hospital surveys of patients that started in 2006 and covers such topics as hospital responsiveness, cleanliness, and the quality of communication between patients and medical staff at the hospital.[39] As a result of this information consumers are now aware that there are very few hospitals that have received five star ratings and will be able to provide the best level of care, 251 out of 3,553 (or seven percent) to be exact.[40]

> "[T]he Commission cannot –and will not- stand idly by when a carrier's lax data security practices expose the personal information of hundreds of thousands of the most vulnerable Americans to identity theft and fraud."

Before this information was released patients did not know the quality of the hospital and therefore the service that they were to receive. This information also revealed that when hospitals were rated for their quality there were very few that received good ratings, and before the ratings the quality of the hospital was probably little known to consumers. Due to this release consumers now have the ability to access information to better their decision-making when choosing a hospital. Hospitals also have an incentive to improve their service because they are now being rated for their performance, and that rating is being communicated to consumers.

One of the newest of these organizations to focus on the risks of new technology and how to better help consumers is the Office of Technology Research and Education, a subset of the Bureau of Consumer Protection within the Federal Trade Commission.[41] Their mandate is to investigate and help inform consumers of new technologies and the various security issues that consumers may face. The office's creation in March 2014 is an expansion of the Mobile Technology Unit of the Federal Trade Commission which had focused on recent advances in mobile technology and their risk.[42] Their dual role in both investigating (and the FTC as the broader organization being able to fine) and educating consumers is a hybrid of past government organizational efforts like the FDA and the FCC. But the latest effort by the FCC with AT&T in regard to enforcement has been unprecedented compared to the TerraCom and YourTel fines.

This most recent case with AT&T emphasizes this new policy by the Federal government to protect consumer privacy. The FCC has set precedence in the cases of AT&T and YourTel/TerraCom, and will undoubtedly continue to pursue it. As FCC Chairman Tom Wheeler stated "[T]oday's action demonstrates, the Commission will exercise its full authority against companies that fail to safeguard the personal information of their customer,"[43] which can best be interpreted as a major policy shift by the FCC, and perhaps the government, against private companies who are lax with their consumers data security. This action is additionally significant because this is the largest enforcement action that the FCC has taken regarding privacy and data security in the history of the FCC.[44] Wheeler said it well "[A]s the nation's expert agency on communications networks, the Commission cannot –and will not– stand idly by when a carrier's lax data security practices expose the personal information of hundreds of thousands of the most vulnerable Americans to identity theft and fraud."[45]

Four months before the FCC settlement, in January of 2015, President Obama, while at the Federal Trade Commission (FTC), highlighted that recent breaches have resulted in over 100 million Americans having their personal data, including credit card information, compromised.[46]

This is a continuation of his policy to focus on cyber issues like cyberwarfare,[47] but is now focusing more on cybersecurity and information sharing between the government and private companies.[48] While at the FTC, the President laid out steps that are being taken to protect American consumers including introducing legislation that would protect consumers' privacy in the form of a "Consumer Privacy Bill of Rights" and legislation that would require companies to notify consumers within 30 days of a breach.[49]

There has clearly been a shift in policy and action by the government, to protect consumers' information. The President as well as the FCC has taken steps to help regain the trust of society, or at the very least reassure society that action will take place to remedy the damage that is taking place. In the past two years important precedents have been set. The President has announced a policy shift pursuing legislation that would protect consumers, the FCC has fined companies for failing to adequately secure their customers personal information, and Medicare has created a rating system to inform consumers about the quality of service that they can receive. Yet more needs to be done.

"[C]ompanies that handle consumer financial data seem to treat cybersecurity and data breaches the same way that the car industry did with vehicle safety decades ago, where safety is ignored and companies do not want to talk about it"

What Else Needs to be Done

There is still a cybersecurity consumer education gap when hundreds of millions of consumers have their financial information entrusted in companies, but do not know how secure their financial information is. It is akin to investing in the bond market without there being any rating of the bonds that a consumer is investing in.

The payment card industry as well as many companies that handle consumer financial data seem to treat cybersecurity and data breaches the same way that the car industry did with vehicle safety decades ago, where safety is ignored and companies do not want to talk about it. There needs to be a fundamental shift in the ways companies deal with cybersecurity. A model of this may be the way the way that manufacturers today advertise the safety of their cars. Payment card companies should do the same and be able to reassure customers by making cybersecurity a point of company pride.

The CFPB should take these recent actions by the Executive branch and their mandate to educate consumers to create a rating system of their own to inform consumers about the how well companies are able to protect consumer information, and how they react to an information breach to protect consumers. A rating system could be used made consisting of letter grades (A, B-, C+, etc.) and act as a company cybersecurity report card (see Figure in Appendix) that reflects the many factors that go into cybersecurity before, during, and after a cyberattack and information breach. A letter grade system is much more preferable due its greater specificity than a one to five star scale that Medicare has used because of the complexity of the information security issue.

This system would work well if there was both an overall grade and an individual grade for all 12 of the areas of the Payment Card Industry Standard.[50] Verizon itself has used this standard in its payment breach investigations for 10 years.[51] This rating system could be posted on either the CFPB's website, or an additional website solely dedicated to this system where consumers can compare companies just as you can with Medicare's hospital ratings system. The Payment Card Industry Standard is a good start for the rating system, and the standards should be improved upon in the future if appropriate. Additionally, the FTC and FCC should continue their current endeavors to inform consumers of the risks of emerging technologies, and go after

companies that fail to secure consumers personal information.

In summary, the market has failed to create a system to address both a lack of cybersecurity and fill the cybersecurity consumer education gap. The government should continue its pledge to protect consumers, and should inform consumers so that they can make better, safer choices for their financial future.

End Notes

[1] Radius Global Market Research, "Market Research Methodology, Market Research Approach." Radius Global Market Research. Last modified April 3, 2014. http://www.radius-global.com/about/news-releases/online-security-a-full-blown-marketing-crisis.
[2] BBC News, "BBC News - Xbox and PlayStation Resuming Service After Attack." BBC News. Last modified December 27, 2014. http://www.bbc.com/news/uk-30602609. I experienced this particular outage over the 2014 Thanksgiving Holiday.
[3] Everett Rosenfeld, "FBI Investigating Central Command Twitter Hack." CNBC. Last modified January 12, 2015. http://www.cnbc.com/id/102330338.
[4] Ibid.
[5] Thomas Fox-Brewster, "DOD, Yahoo Hack Suspects and Alleged Lizard Squad Member Arrested By UK Cops." Forbes. Last modified March 6, 2015. http://www.forbes.com/sites/thomasbrewster/2015/03/06/dod-yahoo-and-lizard-squad-hacker-suspects-arrested-by-uk-cops/.
[6] James Temperton, "UK Hacker Arrested Over Xbox Live and PSN Attacks." Wired UK. Last modified January 16, 2015. http://www.wired.co.uk/news/archive/2015-01/16/playstation-xbox-ddos-arrest.
[7] CNN Money, "Lawsuits Piling Up On Target Over Hack." CNN. Last modified December 24, 2014. http://money.cnn.com/2013/12/23/news/companies/target-credit-card-lawsuits/.
[8] Hiroko Tabuchi, "$10 Million Settlement in Target Data Breach Gets Preliminary Approval." The New York Times. Last modified March 19, 2015. http://www.nytimes.com/2015/03/20/business/target-settlement-on-data-breach.html.
[9] Ibid.
[10] Verizon Enterprise, "2015 PCI Compliance Report," Verizon Enterprise Solutions. Last modified 2015. http://www.verizonenterprise.com/pcireport/2015/ . The report can be accessed via download from this page.
[11] Ibid.
[12] Federal Communications Commission, "$10M Fine Proposed Against TerraCom and YourTel for Privacy Breaches." FCC.gov. Last modified October 24, 2014. http://www.fcc.gov/document/10m-fine-proposed-against-terracom-and-yourtel-privacy-breaches.
[13] Ibid.
[14] Federal Communications Commission, "Lifeline: Affordable Telephone Service for Income-Eligible Subscribers." FCC.gov. Last modified April 8, 2014. http://www.fcc.gov/guides/lifeline-and-link-affordable-telephone-service-income-eligible-consumers.
[15] Federal Communications Commission, "$10M Fine" Proposed Against TerraCom and YourTel for Privacy Breaches." FCC.gov. Last modified October 24, 2014. http://www.fcc.gov/document/10m-fine-proposed-against-terracom-and-yourtel-privacy-breaches.
[16] Ibid.
[17] Federal Communications Commission, "AT&T to pay $25M to settle investigation into three data breaches." FCC.gov. Last modified April 8, 2015. http://www.fcc.gov/document/att-pay-25m-settle-investigation-three-data-breaches-0.
[18] Radius Global Market Research. "Market Research Methodology, Market Research Approach".
[19] Michael Riley, Ben Elgin, Dune Lawrence, and Carol Matlack, "Target Missed Warnings in Epic Hack of Credit Card Data." Bloomberg. Last modified March 13, 2014. http://www.bloomberg.com/bw/articles/2014-03-13/target-missed-alarms-in-epic-hack-of-credit-card-data.

[20] Mark Kuykendall and Rick Wash, "Poor Decision-Making Can Lead to Cybersecurity Breaches." MSUToday Michigan State University. Last modified February 14, 2015. http://msutoday.msu.edu/news/2015/poor-decision-making-can-lead-to-cybersecurity-breaches/.

[21] Federal Financial Institutions Examination Council, "FFIEC Cybersecurity Assessment General Observations." FFIEC. Last modified 2014. http://www.ffiec.gov/press/PDF/FFIEC_Cybersecurity_Assessment_Observations.pdf.

[22] Moore, Tyler, Richard Clayton, and Ross Anderson. "The Economics of Online Crime."*Journal of Economic Perspectives* 23, no. 3 (2009): 3-20. doi:10.1257/jep.23.3.3.

[23] Katherine Campbell, Lawrence A. Gordon, Martin P. Loeb, and Lei Zhou. "The Economic Cost of Publicly Announced Information Security Breaches: Empirical Evidence From the Stock Market." *Journal of Computer Security* 11, no. 3 (2003): 431-448.

[24] Lawrence A. Gordon, Martin P. Loeb, and Tashfeen Sohail, "Market Value of Voluntary Disclosures Concerning Information Security." *Management Information Systems Quarterly* 34, no. 3 (2010): 567-594

[25] Ponemon Institute. "2014 Cost of Data Breach Study: Global Analysis." Ponemon Institute. Last modified May 2014. http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?subtype=WH&infotype=SA&appname=GTSE_SE_SE_USEN&htmlfid=SEL03027USEN&attachment=SEL03027USEN.PDF#loaded.

[26] James Lewis and Stewart Baker, "The Economic Impact of Cybercrime and Cyber Espionage." Center for Strategic and International Studies. Last modified July 2013. http://csis.org/files/publication/60396rpt_cybercrime-cost_0713_ph4_0.pdf.

[27] David Chinn, James Kaplan, and Allen Weinberg. "Risk and Responsibility in a Hyperconnected World: Implications for Enterprises." McKinsey And Company. Last modified January 2014. http://www.mckinsey.com/insights/business_technology/risk_and_responsibility_in_a_hyperconnected_world_implications_for_enterprises

[28] J. D. Lewis and Andrew J. Weigert, "Social atomism, holism, and trust." *Sociological Quarterly* 26, no. 4 (1985): 455-471. doi:10.1111/j.1533-8525.1985.tb00238.x.

[29] Thomas Rid, *Cyber War Will Not Take Place*. 2013, 25.

[30] Nicola Smith, "Marketing Tactics Data Security." Last modified March 6, 2014. http://www.radius-global.com/media/98552/030614_special_report_data_security.pdf.

[31] Radius Global Market Research. "Market Research Methodology, Market Research Approach".

[32] Ibid.

[33] Ibid.

[34] Ibid.

[35] Consumer Financial Protection Bureau, "About Us Consumer Financial Protection Bureau." Consumer Financial Protection Bureau. Last modified December 4, 2014. http://www.consumerfinance.gov/the-bureau/.

[36] Radius Global Market Research, "Market Research Methodology, Market Research Approach".

[37] Food and Drug Administration, "History." U S Food and Drug Administration Home Page. Last modified March 23, 2015. http://www.fda.gov/AboutFDA/WhatWeDo/History/default.htm.

[38] Centers for Medicare & Medicaid Services, "CMS Releases First Hospital Compare Star Ratings." Centers for Medicare & Medicaid Services. Last modified April 16, 2015. https://www.cms.gov/Newsroom/MediaReleaseDatabase/Press-releases/2015-Press-releases-items/2015-04-16.html.

[39] Ibid.

[40] Kaiser Health News, "Hospital Stars for Patient Satisfaction." Kaiser Health News. Last modified April 16, 2015. http://cdn.kaiserhealthnews.org/attachments/HospitalStarsForPatientSatisfaction.pdf. This source aggregates the data. Searching on the Medicare website will only display at most one state at a

time, this source consolidates them into one PDF file. US News and World Report also has an excellent article that describes the rating and has a breakdown of the numbers which I verified with the above with this source, and can be found here: http://www.usnews.com/news/articles/2015/04/17/only-251-hospitals-score-five-stars-in-medicares-new-ratings.

[41] Jessica Rich, "BCP's Office of Technology Research and Investigation: The Next Generation in Consumer Protection." Federal Trade Commission. Last modified March 23, 2015. https://www.ftc.gov/news-events/blogs/business-blog/2015/03/bcps-office-technology-research-investigation-next.

[42] Ibid.

[43] Federal Communications Commission, "AT&T to pay $25M".

[44] Ibid.

[45] Ibid.

[46] White House, "Remarks By The President At The Federal Trade Commission." The White House. Last modified January 12, 2015. https://www.whitehouse.gov/the-press-office/2015/01/12/remarks-president-federal-trade-commission.

[47] The Guardian, "Obama Tells Intelligence Chiefs to Draw Up Cyber Target List." The Guardian. Last modified June 7, 2013. http://www.theguardian.com/world/interactive/2013/jun/07/obama-cyber-directive-full-text.

[48] Dustin Volz, "Responding to Sony Hack, Senate Advances Major Cybersecurity Bill." National Journal. Last modified March 12, 2015. http://www.nationaljournal.com/tech/responding-to-sony-hack-senate-advances-major-cybersecurity-bill-20150312.

[49] White House, "Remarks By The President At The Federal Trade Commission." The White House. Last modified January 12, 2015. https://www.whitehouse.gov/the-press-office/2015/01/12/remarks-president-federal-trade-commission.

[50] PCI Security Standards Council, "PCI Security Standards Documents: PCI DSS, PA-DSS, PED Standards, Compliance Guidelines and More." PCI Security Standards Council Site. Accessed May 5, 2015. https://www.pcisecuritystandards.org/security_standards/documents.php?agreements=pcidss&association=pcidss. I accessed version 3.1, the latest version, from the cited link whereupon you are required to register to download the standards. A direct PDF link can be found here: https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-1.pdf. In it are the extensive guidelines.

[51] Verizon Enterprise, "2015 PCI Compliance Report".

Bibliography

BBC News. "BBC News - Xbox and PlayStation Resuming Service After Attack." BBC News. Last modified December 27, 2014. http://www.bbc.com/news/uk-30602609.

Campbell, Katherine, Lawrence A. Gordon, Martin P. Loeb, and Lei Zhou. "The Economic Cost of Publicly Announced Information Security Breaches: Empirical Evidence From the Stock Market." *Journal of Computer Security* 11, no. 3 (2003): 431-448.

Centers for Medicare & Medicaid Services. "CMS Releases First Hospital Compare Star Ratings." Centers for Medicare & Medicaid Services. Last modified April 16, 2015. https://www.cms.gov/Newsroom/MediaReleaseDatabase/Press-releases/2015-Press-releases-items/2015-04-16.html.

Chinn, David, James Kaplan, and Allen Weinberg. "Risk and Responsibility in a Hyperconnected World: Implications for Enterprises." McKinsey And Company. Last modified January 2014. http://www.mckinsey.com/insights/business_technology/risk_and_responsibility_in_a_hyperconnected_world_implications_for_enterprises.

CNN Money. "Lawsuits Piling Up On Target Over Hack." CNN. Last modified December 24, 2014. http://money.cnn.com/2013/12/23/news/companies/target-credit-card-lawsuits/.

Consumer Financial Protection Bureau. "About Us Consumer Financial Protection Bureau." Consumer Financial Protection Bureau. Last modified December 4, 2014. http://www.consumerfinance.gov/the-bureau/.

Federal Communications Commission. "Lifeline: Affordable Telephone Service for Income-Eligible Subscribers." FCC.gov. Last modified April 8, 2014. http://www.fcc.gov/guides/lifeline-and-link-affordable-telephone-service-income-eligible-consumers.

Federal Communications Commission. "$10M Fine Proposed Against TerraCom and YourTel for Privacy Breaches." FCC.gov. Last modified October 24, 2014. http://www.fcc.gov/document/10m-fine-proposed-against-terracom-and-yourtel-privacy-breaches.

Federal Communications Commission. "AT&T to pay $25M to settle investigation into three data breaches." FCC.gov. Last modified April 8, 2015. http://www.fcc.gov/document/att-pay-25m-settle-investigation-three-data-breaches-0.

Federal Financial Institutions Examination Council. "FFIEC Cybersecurity Assessment General Observations." FFIEC. Last modified 2014. http://www.ffiec.gov/press/PDF/FFIEC_Cybersecurity_Assessment_Observations.pdf.

Food and Drug Administration. "History." U S Food and Drug Administration Home Page. Last modified March 23, 2015. http://www.fda.gov/AboutFDA/WhatWeDo/History/default.htm.

Fox-Brewster, Thomas. "DOD, Yahoo Hack Suspects and Alleged Lizard Squad Member Arrested By UK Cops." Forbes. Last modified March 6, 2015. http://www.forbes.com/sites/thomasbrewster/2015/03/06/dod-yahoo-and-lizard-squad-hacker-suspects-arrested-by-uk-cops/.

Gordon, Lawrence A., Martin P. Loeb, and Tashfeen Sohail. "Market Value of Voluntary Disclosures Concerning Information Security." *Management Information Systems Quarterly* 34, no. 3 (2010): 567-594.

Kaiser Health News. "Hospital Stars for Patient Satisfaction." Kaiser Health News. Last modified April 16, 2015. http://cdn.kaiserhealthnews.org/attachments/HospitalStarsForPatientSatisfaction.pdf.

Kuykendall, Mark, and Rick Wash. "Poor Decision-Making Can Lead to Cybersecurity Breaches." MSUToday Michigan State University. Last modified February 14, 2015. http://msutoday.msu.edu/news/2015/poor-decision-making-can-lead-to-cybersecurity-breaches/.

Lewis, J. D., and Andrew J. Weigert. "Social atomism, holism, and trust." *Sociological Quarterly* 26, no. 4 (1985): 455-471. doi:10.1111/j.1533-8525.1985.tb00238.x.

Lewis, James, and Stewart Baker. "The Economic Impact of Cybercrime and Cyber Espionage." Center for Strategic and International Studies. Last modified July 2013. http://csis.org/files/publication/60396rpt_cybercrime-cost_0713_ph4_0.pdf.

Moore, Tyler, Richard Clayton, and Ross Anderson. "The Economics of Online Crime."*Journal of Economic Perspectives* 23, no. 3 (2009): 3-20. doi:10.1257/jep.23.3.3.

PCI Security Standards Council. "PCI Security Standards Documents: PCI DSS, PA-DSS, PED Standards, Compliance Guidelines and More." PCI Security Standards Council Site. Accessed May 5, 2015. https://www.pcisecuritystandards.org/security_standards/documents.php?agreements=pcidss&association=pcidss.

Ponemon Institute. "2014 Cost of Data Breach Study: Global Analysis." Ponemon Institute. Last modified May 2014. http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?subtype=WH&infotype=SA&appname=GTSE_SE_SE_USEN&htmlfid=SEL03027USEN&attachment=SEL03027USEN.PDF#loaded.

Radius Global Market Research. "Market Research Methodology, Market Research Approach." Radius Global Market Research. Last modified April 3, 2014. http://www.radius-global.com/about/news-releases/online-security-a-full-blown-marketing-crisis.

Rich, Jessica. "BCP's Office of Technology Research and Investigation: The Next Generation in Consumer Protection." Federal Trade Commission. Last modified March 23, 2015. https://www.ftc.gov/news-events/blogs/business-blog/2015/03/bcps-office-technology-research-investigation-next.

Rid, Thomas. *Cyber War Will Not Take Place*. 2013.

Riley, Michael, Ben Elgin, Dune Lawrence, and Carol Matlack. "Target Missed Warnings in Epic Hack of Credit Card Data." Bloomberg. Last modified March 13, 2014. http://www.bloomberg.com/bw/articles/2014-03-13/target-missed-alarms-in-epic-hack-of-credit-card-data.

Rosenfeld, Everett. "FBI Investigating Central Command Twitter Hack." CNBC. Last modified January 12, 2015. http://www.cnbc.com/id/102330338.

Smith, Nicola. "Marketing Tactics Data Security." Last modified March 6, 2014. http://www.radius-global.com/media/98552/030614_special_report_data_security.pdf.

Tabuchi, Hiroko. "$10 Million Settlement in Target Data Breach Gets Preliminary Approval." The New York Times. Last modified March 19, 2015. http://www.nytimes.com/2015/03/20/busi

ness/target-settlement-on-data-breach.html.

Temperton, James. "UK Hacker Arrested Over Xbox Live and PSN Attacks." Wired UK. Last modified January 16, 2015. http://www.wired.co.uk/news/archive/2015-01/16/playstation-xbox-ddos-arrest.

The Guardian. "Obama Tells Intelligence Chiefs to Draw Up Cyber Target List." The Guardian. Last modified June 7, 2013. http://www.theguardian.com/world/interactive/2013/jun/07/obama-cyber-directive-full-text.

Verizon Enterprise. "2015 PCI Compliance Report." Verizon Enterprise Solutions. Last modified 2015. http://www.verizonenterprise.com/pcireport/2015/.

Volz, Dustin. "Responding to Sony Hack, Senate Advances Major Cybersecurity Bill." National Journal. Last modified March 12, 2015. http://www.nationaljournal.com/tech/responding-to-sony-hack-senate-advances-major-cybersecurity-bill-20150312.

White House. "Remarks By The President At The Federal Trade Commission." The White House. Last modified January 12, 2015. https://www.whitehouse.gov/the-press-office/2015/01/12/remarks-president-federal-trade-commission.

Appendix

Figure Example of a CFPB report card.

Example Company's CFPB Cybersecurity Rating. Final Grade: **C-**		
Control Objectives:	**PCI DSS Requirements:**	**Grade:**
Build and Maintain a Secure Network and Systems	1. Install and maintain a firewall configuration to protect cardholder data	A-
	2. Do not use vendor-supplied defaults for system passwords other security parameters	C
Protect Cardholder Data	3. Protect stored cardholder data	D+
	4. Encrypt transmission of cardholder data across open, public networks	D
Maintain a Vulnerability Management Program	5. Protect all systems against malware and regularly update anti-virus software or programs	C
	6. Develop and maintain secure systems and applications	B-
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need to know	D+
	8. Identify and authenticate access to system components	C
	9. Restrict physical access to cardholder data	B+
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data	C
	11. Regularly test security systems and processes	F
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for all personnel	C

Source: Adapted from "PCI DSS Version 3.1," *Pcisecuritystandards.org.* Accessed May 8. 2015. https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-1.pdf.