Journal of International Business and Law

Volume 16 | Issue 1 Article 10

5-1-2016

Cyber Security: Bull's-Eye on Small Businesses

Jane Chen
Maurice A. Deane School of Law at Hofstra University

CYBER SECURITY: BULL'S-EYE ON SMALL BUSINESSES

By Jane Chen[*]

I. INTRODUCTION

In the past decade, the Internet has become an indispensable tool for the business world. Businesses of all sizes are heavily relying on cloud-based systems and various virtual applications such as Email, Twitter, and Facebook for management purposes, among others. In fact, it is a preferred medium to communicate, conduct transactions, and share information,[1] regardless of where that individual is located, as long as they have a source of Internet connection.[2] Innovative technology plays a major role in the success of a business and puts a competitive edge to business models, but they can also be the crux of business failures.[3]

Cyber security breach has become one of the most difficult obstacles business owners have to face for a variety of reasons.[4] The key is preparation. Small businesses generally do not believe they will be the victims of a cyber security breach.[5] Budgets are allocated to the management and maintenance of the business and business owners have little flexibility or desire to devote valuable resources to speculative risks that may not even occur.[6] This is demonstrated in the 2013 Target data breach.[7]

The Target Corporation, one of the largest retailers in the United States, experienced an unprecedented cyber breach in 2013.[8] As a result of the breach, 70 million customers' data, such as credit card information, name, address, and phone number were compromised.[9] They suffered approximately $252 Million in expenses relating to the 2013 breach[10] and ultimately

---

[*] J.D. Candidate, Maurice A. Deane School of Law at Hofstra University, 2017.

[1] Frank Newport, *The New Era of Communication Among Americans*, GALLUP (Nov. 10, 2014), http://www.gallup.com/poll/179288/new-era-communication-americans.aspx.

[2] *See id.*

[3] *See generally* Robert Strohmeyer, *Hackers Put a Bull's-eye on Small Business*, PCWORLD (Aug. 12, 2013), http://www.pcworld.com/article/2046300/hackers-put-a-bulls-eye-on-small-business.html.

[4] *See generally* Kevin McCarthy, *Cybersecurity for the 21st Century*, MAJORITY LEADER (Apr. 22, 2015), http://www.majorityleader.gov/2015/04/22/cybersecurity-21st-century.

[5] *See* John Brandon, *Why Your Business Might Be a Perfect Target for Hackers*, INC., http://www.inc.com/magazine/201312/john-brandon/hackers-target-small-business.html.

[6] Joe Curtis, *Cyber Security not a priority for SMBs, research shows*, ITPRO (Feb. 26, 2015), http://www.itpro.co.uk/security/24126/cyber-security-not-a-priority-for-smbs-research-shows.

[7] *See* Michael Riley, Ben Elgin, Dune Lawrence, and Carol Matlack, *Missed Alarms and 40 Million Stolen Credit Card Numbers: How Target Blew It*, BLOOMBERG BUSINESS (Mar. 13, 2014), http://www.bloomberg.com/bw/articles/2014-03-13/target-missed-alarms-in-epic-hack-of-credit-card-data (outlining the events of the Target breach).

[8] *See* Natalie Gagliordi, *The Target breach, two years later*, ZDNET (Nov. 27, 2015), http://www.zdnet.com/article/the-target-breach-two-years-later.

[9] *See id.*

[10] Kevin M. McGinty, *Target Data Breach Price Tag: $252 Million and Counting*, MINTZ LEVIN (Feb. 26, 2015), https://www.privacyandsecuritymatters.com/2015/02/target-data-breach-price-tag-252-million-and-counting.

forced the CEO of the corporation, Gregg Steinhafel, to resign from the corporation.[11] Despite the remediation efforts, Target will forever be associated with the data breach and its lasting repercussion.[12] This attack was facilitated when the hackers gained access to Target's network on November 27, 2013 through a small vendor, Fazio Mechanical Services (hereinafter, "Fazio").[13] Target contracted with Fazio for providing refrigeration and HVAC systems.[14]

After further investigation, it turns out Fazio's primary method of detecting malicious software on its network was the free version of Malwarebytes Anti-Malware.[15] No other cyber security measures were taken by Fazio.[16] Here, the cyber attackers used phishing emails to trick a Fazio employee to click on the email and download Citadel, a password stealing bot.[17] With minimum effort by the cyber attackers, Citadel was able to successfully obtain Fazio's login credentials to the Target's vendor portal.[18] After which they took control of their internal networks, gaining access to millions of customer personal data.[19] Fazio was one of the small businesses that were not subject to regulation by the government in regards to cyber security, however after the breach, the legislature contemplated and discusses whether the government should play a role in requiring companies to adopt updated data security technologies.[20] Despite the lack of regulations, they were still doing business with one of the largest corporation in the nation. Accordingly, cyber hackers count on the small businesses that are generally unprepared and unarmed so they can be used as a bait to catch the bigger fish in the sea.

Overall, cyber security breaches pose not only a national concern, but also cause massive damage on an international level. U.S. companies from both the pharmaceutical and technology industry are attractive targets to foreign countries such as China, North Korea, and Russia.[21] President Barack Obama has made initiatives to tame the situation, one of which was by forming a cyber agreement with China.[22] However, investigators from security firms indicate cyber-attacks are still recurrent and ongoing from sources linked to the China based

---

[11] Clare O'Connor, *Target CREO Gregg Steinhafel Resigns In Data Breach Fallout,* FORBES (May 5, 2014), http://www.forbes.com/sites/clareoconnor/2014/05/05/target-ceo-gregg-steinhafel-resigns-in-wake-of-data-breach-fallout/#6207481c6e61.

[12] *See* Gagliordi, *supra* note 8.

[13] *See* Maggie McGrath, *Target Data Breach Spilled Info On As Many As 70 Million Customers,* FORBES (Jan. 10, 2014), http://www.forbes.com/sites/maggiemcgrath/2014/01/10/target-data-breach-spilled-info-on-as-many-as-70-million-customers/#58d1f7fa6bd1.

[14] *See* Brian Krebs, *Email Attack on Vendor Set Up Breach at Target,* KREBS ON SECURITY (Feb. 14, 2014), http://krebsonsecurity.com/2014/02/email-attack-on-vendor-set-up-breach-at-target.

[15] *See id.*

[16] *See id.*

[17] *See* Gagliordi, *supra* note 8.

[18] *See id.*

[19] *See id.*

[20] *See* N. Eric Weiss and Rena S. Miller, The Target and Other Financial Data Breaches: Frequently Asked Questions, CONGRESSIONAL RESEARCH SERVICE (Feb. 4, 2015), https://www.fas.org/sgp/crs/misc/R43496.pdf.

[21] Dan Worth, *Russia, China, North Korea and Iran remain top US cyber concerns,* V3CO (Sept. 11, 2015), http://www.v3.co.uk/v3-uk/news/2425633/russia-china-north-korea-and-iran-remain-top-us-cyber-concerns.

[22] *See* Teresa Welsh, *Obama, Xi Reach Agreement to End Cyberattacks,* U.S. NEWS (Sept. 25, 2015), http://www.usnews.com/news/articles/2015/09/25/president-obama-chinese-president-xi-jingping-announce-agreement-to-stop-hacking.

firms.[23] Dr. Ziv Chang, senior director of Cyber Safety Solutions at Trend Micro, believes the "China based Iron Tiger hacking group is a highly active, continuously advanced, persistent threat that continues to attack the U.S."[24] However, China is not the only country that poses a persistent threat to the U.S.[25] These foreign countries are ambitious and have their eyes on more than just American consumer's personal data. Historically, they've stolen emails, intellectual property, and strategic planning documents.[26]

This note will discuss the various regulations currently in place and the changes necessary to ensure compliance among business owners. Since 2002, no major cyber security legislation has been enacted.[27] Although there are laws that address certain aspects of cyber security, the nation lacks an overarching framework that addresses this issue.[28] The lack of enforceable regulations gives smaller businesses less motivation to exercise caution and become better prepared for the inevitable to occur: cyber-attacks.[29] In order to remedy this issue, solutions, provided herein, should be adopted by the legislature and provide small business not merely optional guidelines to be practiced, but also agency oversight to ensure that the small businesses are in compliance. Taken into account small businesses have limited monetary resources, the solutions will not financially burden the small business owners. Instead the proposed mandatory acts will minimize the risk of cyber security at little cost, so long as the employers and employees of the small businesses perform their due diligence.

In addition to intra-national cyber security concerns, cyber-attacks come from not only within the nation, but also from foreign countries, such as China, that attempts to steal a company's innovative ideas or formulas.[30] Nonetheless, incentivizing the business owners to act prior to the cyber-attack will minimize those risks and damages that would result if the breach were actually to occur. There is a large percentage of non-compliance of small businesses to the guidelines, which demonstrates the need to intervene and put those guidelines into practice to mitigate damages and to minimize the percentage of business failures in the wake of a cyber breach.[31] The threshold for designation of small businesses is

---

[23] Lisa Brownlee, *China-based Cyber Attacks On US Military Are 'Advanced, Persistent And Ongoing': Report,* FORBES (Sept. 17, 2015), http://www.forbes.com/sites/lisabrownlee/2015/09/17/chinese-cyber-attacks-on-us-military-interests-confirmed-as-advanced-persistent-and-ongoing/#3f797ee41809.

[24] *See id.*

[25] *See* Worth, *supra* note 21.

[26] *See id.*

[27] *See generally* Eric A. Fischer, *Federal Laws Relating to Cybersecurity: Overview and Discussion of Proposed Revisions*, CONGRESSIONAL RESEARCH SERVICE (June 20, 2013), https://www.fas.org/sgp/crs/natsec/R42114.pdf (stating that despite its complexity, there is no overarching framework legislation from the U.S government in addressing cybersecurity).

[28] *See id.*

[29] *See generally* Brian Honan, *Making your Business Cyber Resilient*, SECURITY INTELLIGENCE (Dec. 12, 2014), https://securityintelligence.com/making-your-business-cyber-resilient.

[30] Joseph Menn, *China tried to hack U.S. firms even after cyber pact: CrowdStrike*, REUTERS (Oct. 19, 2015), http://www.reuters.com/article/us-usa-china-cybersecurity-idUSKCN0SD0AT20151020.

[31] Paula Fernandes, *Essential Steps for Improving Your Small Business Cybersecurity*, BUSINESS NEWS DAILY (June 16, 2016) http://www.businessnewsdaily.com/6058-improve-small-business-cybersecurity.html.

broad and provides little accountability for those businesses to face consequences for their lack of due diligence to protect the information of their clients and their reputation.[32]

II. BACKGROUND

A. Small Businesses as the Primary Target

In an April 2015 press release, the Small Business Committee cites that "71 percent of cyber-attacks occur at businesses with fewer than 100 employees."[33] Generally, small businesses are marked as a target for cyber-attacks for a many reasons. First, small businesses are much easier to attack than larger organizations.[34] Specifically as there are few small businesses that allocate funds and resources, such as expert personnel, in attempts of mitigating the risks that cyber-attacks pose.[35] In fact, a majority of the small business owners lack the knowledge and expertise to keep up with the problems caused by an increasing dependency on Internet platforms.[36] A study conducted by security provider, Norton by Symantec, shows that less than one-third of small businesses understand how to combat cyber criminals.[37] Furthermore, only 28% of the small businesses actually have a plan in place to respond to cyber-attacks.[38] Consequently, 60% of small businesses fail within six months of a data breach.[39]

The Small Business Committee designates what constitute an appropriate size for small businesses.[40] Typically, small businesses consist of 500 employees or less.[41] Small businesses are the foundation of the United States economy. Over the past ten years, they were consistently responsible for 60% to 80% of net new job creations.[42] Furthermore, in 2012 the U.S. Census Bureau data reported, small businesses represent 99.7 % of all the

---

[32] *See generally,* Testimony of Gregory C. Wilshusen, Director, Government Accountability Office, before the Subcommittees on Research and Technology and Oversight, Committee on Science, Space and Technology, House of Representatives (July 8, 2015), http://www.gao.gov/assets/680/671253.pdf.

[33] Press Release, Small Business Committee, Small Business, Big Threat: protecting Small Businesses from Cyber Attacks (Apr. 22, 2015), http://smallbusiness.house.gov/news/documentsingle.aspx?DocumentID=398099.

[34] *See* Sammi Caramela, Cybersecurity: A Small Business Guide, BUSINESS NEWS DAILY (July 28, 2015), http://www.businessnewsdaily.com/8231-small-business-cybersecurity-guide.html.

[35] *See* Anthony Sills, *Protect Your Business from a Data Security Breach*, BUSINESS KNOW HOW (2014), http://www.businessknowhow.com/technology/datasecurity.htm.

[36] *See id.*

[37] Fernandes, *supra* note 31.

[38] *Id.*

[39] *See id.*; Strohmeyer, *supra* note 3 (according to a research study conducted by the National Cyber Security Alliance team).

[40] *See* Table of Small Business Size Standards, U.S. SMALL BUSINESS ADMINISTRATION, https://www.sba.gov/content/small-business-size-standards.

[41] *See* Richard Kissel, *Small Business Information Security: The Fundamentals*, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (Oct. 2009), http://csrc.nist.gov/publications/nistir/ir7621/nistir-7621.pdf.

[42] *See* Letter from Fred Upton, Chairman, Committee on Small Business, Steven Chabot, Chairman, Committee on Energy and Commerce, et al., to Thomas Wheeler, Chairman, Federal Communications Commission (Nov. 19, 2015), http://energycommerce.house.gov/sites/republicans.energycommerce.house.gov/files/114/Letters/20151119FCC.pdf.

employers in the nation. If non-employer businesses with less than 500 employees were added; the percentage increases to 97.9%.[43] The employer's level of diligence to the protect customer's private information should increase based on the number of employees they employ. This is because the numbers of employees reflect on the amount of businesses they conduct, and consequently the amount of non-public information that they hold. To allow a great majority of business in our nation to be designated as small businesses makes it difficult to regulate. To illustrate, the attentiveness of an employer with 20 employees should not be equivalent to that of an employer with 450 employees. The level of regulations needs to be commensurate with the size of the business.[44] The publications of voluntary guidelines are insufficient to compel compliance and prepare for cyber security threats.[45]

In a survey study, conducted in April 2015, containing 400 small businesses, 27% of those do not have a security protocols in place, while 26% failed to back up their data on a regular basis, a basic guidance in cyber defense.[46] These statistics illustrate how small businesses overlook the importance of developing cyber security defense. Instead, they tend to focus more on the growth and development of their core business. Although this exemplifies great entrepreneurship, they are gambling away the reputation of their business, as well as the privacy of their customers when they neglect the importance of these issues. Hence, awareness and education is essential is countering the rapidly evolving threat of cyber-crime.[47]

Large businesses and organizations are generally more prepared to face the aftermath of cyber-attacks. This is because large businesses have more to risk due to their extended clientele records, and have a greater source of revenue. As compared to small businesses, cyber criminals are less prone to attack these larger organizations, as it would require a great investment to hack through their multiple levels of security protection. However, these larger organizations do have both a direct and indirect business relationships with these smaller businesses. The relationship between these two is a vendor-relationship. Here, large organizations contract independent businesses specializing in a particular service they need.

---

[43] *See* Small Business Facts and Data, SMALL BUSINESS & ENTREPRENEURSHIP COUNCIL, http://sbecouncil.org/about-us/facts-and-data.

[44] *See generally* Michael Daniel, Assessing Cyber security Regulations, THE WHITE HOUSE (May, 22, 2014), https://www.whitehouse.gov/blog/2014/05/22/assessing-cybersecurity-regulations.

[45] *See id.* (recommending that the guidelines been complimented by regulations to mitigate the risks of cyber attacks).

[46] Press Release, Time Warner Cable, Security and New Technology upgrades a Challenge for Small Business Owners According to Time Warner Cable Business Class Small Business Survey (May 2015), https://business.timewarnercable.com/resource-center/news/national-small-business-survey-press-release-twcbc.html (hereinafter, "TWC Press Release").

[47] *See generally* Testimony of William Noonan, Deputy Special Agent, U.S. Secret Service Criminal Investigation Division Cyber Operations Branch, before the House Committee on Homeland Security, Subcommittee on Cybersecurity, Infrastructure Protection and Security Technologies (Feb. 12, 2015), http://www.dhs.gov/news/2015/02/12/written-testimony-usss-house-homeland-security-subcommittee-cybersecurity.

Cyber criminals are targeting small businesses as a gateway into a large organization database, since the security defense is much weaker than that of a larger organization.[48] Large organizations are considered to be the "sprawling network of interconnected vendors".[49] Moreover, the attack of any one vendor can lead to hundreds of millions of dollars.[50] Certain cost in response to a cyber breach may not be avoidable, such as the notification law imposed by the states.[51] Security Breach Notification Laws "require private, governmental or educational entities to notify individuals of security breaches of information involving personally identifiable information."[52] The average cost of such notifications is well over $130 per person.[53] Thus, if the business consists of 1,000 customers in their record, they must notify all those customers whose information may have been compromised, which would yield well over $130,000 on notification requirements alone.[54]

B. Business Closures due to Cyber Breach

As previously discussed, nearly 60% of small businesses fail within six months of being hacked.[55] Code Spaces is one such business that was forced to shut down due to the unsustainable financial responsibility that resulted from the breach.[56] Code Space was a provider of Software as a Service ("SaaS") used by corporations for project management and development needs. SaaS is a software distribution platform where the vendors would host and manage the applications for customers over the Internet.[57] Following the breach, Code Space tracked down the hacker, but was told the company needed to pay a ransom in order to stop the traffic flood damages, but Code Space did not comply.[58] Code Space later announced that:

> [It] will not be able to operate beyond this point, the cost of resolving this issue to date and the expected cost of refunding customers who have been

---

[48] *See* Luis A. Aguilar, The Need for Greater Focus on the Cybersecurity Challenges Facing Small and Midsize Businesses, U.S. Securities and Exchange Commission (Oct. 19, 2015), http://www.sec.gov/news/statement/cybersecurity-challenges-for-small-midsize-businesses.html#_ednref7.

[49] Nicole Perlroth, *Heat System Called Door to Target for Hackers,* N.Y. TIMES (Feb. 5, 2014), http://www.nytimes.com/2014/02/06/technology/heat-system-called-door-to-target-for-hackers.html?_r=1.

[50] *Id.*

[51] *See generally* Security Breach Notification Laws, NATIONAL CONFERENCE OF STATE LEGISLATURES (Oct. 22, 2015), http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.

[52] *See id.*

[53] Kissel, *supra* note 41.

[54] *Id.*

[55] Strohmeyer, *supra* note 3 (citing the National Cyber Security Alliance).

[56] Steve Ragan, *Code Spaces forced to close its doors after security incident,* CSO (June 18, 2014), http://www.csoonline.com/article/2365062/disaster-recovery/code-spaces-forced-to-close-its-doors-after-security-incident.html.

[57] *See* Software as a Service (SaaS) Definitions, TECHTARGET, http://searchcloudcomputing.techtarget.com/definition/Software-as-a-Service.

[58] *See* Ragan, *supra* note 56.

> left with the service they paid for will put Code Space in an irreversible position both financially and in terms of ongoing credibility.[59]

The consequences faced by Code Space due to a cyber security breach serve as a wakeup call for businesses that have critical assets on cloud services.[60]

Another business entity that was forced to shut down due to a series of cyber-attacks was MyBizHomepage.[61] MyBizHomepage was a web-based service that provided small business with tools such as financial analytics and essential information to help them run smoothly.[62] Prior to the breach, the company was valued at $100 million.[63] Yet, throughout the course of business, a disagreement arose between the executive boards.[64] This disagreement resulted in the chief executive officer firing the chief technology officer, along with two other senior officers.[65] As a result of their termination, the three officers sought revenge and launched a series of cyber-attacks that crippled the site.[66] Consequently, the company spent over $1 million to resolve the breach, but ultimately decided that the site had been rendered useless and should be taken down.[67]

C. Important Terms Defined

Cyber Security

Cyber security is the process or measures taken to protect information and systems from major cyber threats.[68] These threats include: cyber terrorism and cyber espionage, among others.[69] This information, which is confidential or proprietary to the corporations, is protected from and defended against unauthorized use, modification, or exploitation.[70] After the Target cyber security breach in 2013, which compromised the personal information of over 70 million customers, large businesses have delegated more funds into cyber breach

---

[59] Michael Mimoso, *Hacker puts Hosting Service Code Spaces Out of Business,* THREAT POST (June 18, 2014), https://threatpost.com/hacker-puts-hosting-service-code-spaces-out-of-business/106761.

[60] *See id.*

[61] *See 3 Companies that Went Out of Business Due to a Security Breach*, PROTECHNOLOGIES (Nov. 6, 2014), https://prooncall.com/3-companies-went-business-due-security-breach.

[62] *MyBizHomepage Launches New Platform to Help Small Businesses*, BUSINESS WIRE (Aug. 6, 2008), http://www.businesswire.com/news/home/20080806006074/en/MyBizHomepage-Launches-Platform-Small-Businesses.

[63] *See* Darren Dahl, *Starting Over After a Cyberattack Shuts Down the Business*, N.Y. TIMES (Aug. 29, 2012), http://boss.blogs.nytimes.com/2012/08/29/starting-over-after-a-cyberattack-shuts-down-the-business.

[64] *See id.*

[65] *Id.*

[66] *Id.*

[67] *Id.*

[68] ProTechnologies, *supra* note 61.

[69] *See* PALOALTO NETWORKS, *What is Cyber Security?*, https://www.paloaltonetworks.com/resources/learning-center/what-is-cyber-security.html.

[70] A Glossary of Common Cybersecurity Terminology, NATIONAL INITIATIVE FOR CYBERSECURITY CAREERS AND STUDIES, https://niccs.us-cert.gov/glossary.

defense.[71] Although actions were taken, many were still victims of the cyber-crimes. In 2014 alone, 233 million customer records were stolen from EBay, 56 million customers had their credit card information stolen from Home Depot, and 76 million customers' data from JPMorgan and Chase were also compromised.[72]

Data Breach

Data breach is one of the consequences of a failed cyber security. More specifically, data breach is the unauthorized movement or disclosure of private information to a party that is outside the organization and unauthorized to possess or see the information.[73] In this generation where our society is transitioning from the storage of tangible documents to an Internet platform, any company that possesses confidential information is at risk of a data breach. Accordingly, those companies are subject to increased risk liability.[74]

Governmental departments are not immune from data breaches. To demonstrate this point, in May 2015, Internal Revenue Service ("IRS") revealed that hackers made 200,000 attempts to access taxpayer personal information using the "get transcript" application.[75] The application itself is an interactive program that allows taxpayers to obtain copies of their own federal tax returns from prior years. Here, information such as birth dates, addresses, and social security numbers are on file for the taxpayer's reference.[76] IRS investigation indicated that approximately 330,000 people were affected as a result of this large breach.[77] Following the breach, the hackers used this information to file fraudulent tax returns.[78] As a result, these hackers made over $39 million by filing these fraudulent tax returns.[79] To remediate this problem, the IRS worked together with private tax preparation firms to seek insight on how to strengthen their computer security system to prevent future cyber-attacks.[80] The IRS further contacted every taxpayer whose data might have been compromised in the mist of the cyber breach.[81] Accordingly, this attack caused immeasurable reputational and monetary damages to the IRS[82]

---

71 *See* Cadie Thompson, *As cyberthreats increase, big money chases patches,* CNBC (Nov. 21, 2014), http://www.cnbc.com/2014/11/21/a-bad-year-for-cybersecurity-but-a-great-one-for-business.html.

72 *See id.* (citing the Identity Theft Resource Center).

73 A Glossary of Common Cybersecurity Terminology, NATIONAL INITIATIVE FOR CYBERSECURITY CAREERS AND STUDIES, https://niccs.us-cert.gov/glossary (stating a data breach could also be conducted by an individual who is outside the organization).

74 *See* Ken Ross, *Cyber Claims Landscape: Companies Face Increasing Data Breach Liability,* http://blog.willis.com/2015/07/cyber-claims-landscape-companies-face-increasing-data-breach-liability.

75 *See* Kevin McCoy, IRS: *Cyber-thieves stole up to $39M,* USA TODAY (June 2, 2015), http://www.usatoday.com/story/money/2015/06/02/irs-data-breach-senate-hearing/28353983.

76 *See* Keith Collins, *A Rare Detailed Look Inside the IRS's Massive Data Breach, via a Security Expert Who Was a Victim* (Aug. 27, 2015), https://qz.com/445233/inside-the-irss-massive-data-breach.

77 *See* Jonathan Vanian, *IRS sued over data breach that affected 330,000 people,* FORTUNE (Aug. 21, 2015), http://fortune.com/2015/08/21/irs-sued-data-breach.

78 *See* McCoy, *supra* note 75.

79 *See id.*

80 *See id.*

81 *Id.*

82 *See generally id.*

Personal Identifiable Information ("PII")

Private Personal Information, also referred to as PII, is a category of sensitive information that can be used to uniquely identify, contact, or locate a particular individual.[83] PII is not information available to the general public.[84] Some examples of PII include: name, address, social security number, telephone number, and any number or code that identifies the individual, such as a bank account number.[85] As a comparison, non-sensitive PII includes: office location, business telephone number, business email address, badge number, and all other information that is reasonable accessible by the public.[86] Generally, cyber hacker target an individual's PII in order to gain access to an individual's accounts, which can result in substantial harm to the individual such as identity thief, or the fraudulent use of their information to make a profit.[87]

III. PROBLEMS

A. Trend of Cyber Security Breaches

John Chambers, Chairman and CEO of Cisco, stated: "There are two types of companies: those who have been hacked, and those who don't yet know they have been hacked."[88] In 2014, three major cyber-attacks shook the corporate world: Target, announcing in January hackers stole PPI from approximately 110 million accounts; JP Morgan Chase who in August experienced a cyber-attack which resulted in approximately 83 million accounts being compromised; and Home Depot who experienced a breach in their payment system in September 2014, resulting in approximately 56 million compromised accounts.[89]

Although small businesses don't make the headlines, there is an industry consensus that both "[s]mall and midsized businesses are now the preferred targets for cybercriminals."[90] The main reason these small businesses are more attractive targets are due to their lack of a strong infrastructure to prevent cyber breaches.[91] This allows cyber criminals to utilize the modern software to produce numerous attacks at once for little investment.[92]

---

[83] Definition of Private Personal Information, UNIVERSITY OF MICHIGAN, http://safecomputing.umich.edu/dataguide/?q=node/89.

[84] *See id.*

[85] *See* UNITED STATES DEPARTMENT OF LABOR, *Guidance on the Protection of Personal Identifiable Information*, http://www.dol.gov/dol/ppii.htm.

[86] *See* UNITED STATES DEPARTMENT OF THE NAVY, *What is Personally Identifiable Information?* (July 15, 2011), http://www.doncio.navy.mil/ContentView.aspx?id=2428.

[87] *See id.*

[88] John Chambers, *What does the Internet of Everything mean for security?*, WORLD ECONOMIC FORUM, https://agenda.weforum.org/2015/01/companies-fighting-cyber-crime/?utm_content=bufferb0881&utm_medium=social&utm_source=facebook.com&utm_campaign=buffer.

[89] Sharone Tobias, *2014: The year in Cyberattcks,* NEWSWEEK (Dec. 31, 2014), http://www.newsweek.com/2014-year-cyber-attacks-295876.

[90] Taylor Armerding, *Why criminals pick on small business,* CSO, http://www.csoonline.com/article/2866911/cyber-attacks-espionage/why-criminals-pick-on-small-business.html.

[91] *Id.*

[92] *Id.*

Unlike large businesses, which are better defended through their frequent updates to firewall protection and viruses, cyber criminals utilize automated attacks to send viruses or ransomware to small business that lack such defense infrastructures.[93] These cyber criminals also have the ability to hack thousands or millions of records at once.[94]

The cyber security industry refers to easy business targets as the "low-hanging fruits."[95] These "low-hanging fruits" are those business that uses minimal effort to protect their computer system.[96] Businesses categorized as a low-hanging fruit fail to perform their due diligence such as regularly changing their passwords, setting requirements for passwords (i.e., using combination of symbols or upper/lower case letters), backing up their system, and informing the employees of security measures.[97] Educating employees on security measures prevent phishing expeditions by the cyber criminals, who send emails with links, or files for the employees to download.[98] Opportunistic criminals tend to choose the path that required the least amount of effort, thus they tend to choose the low-hanging fruits.[99]

B. The Target Data Breach Nightmare

Businesses suffer more than the additional expenses of the breach response, such as a tainted reputation of their business.[100] A survey conducted in 2015 with 2000 respondents, revealed that 86.55% of those respondent would not continue to conduct business with a company that experienced a breach, especially if they failed to protect customers' card data.[101] Tim Critchley, CEO of Semafone, explains that the statistics from this survey demonstrates how "the reputational damage suffered by companies who fail to protect personal data can translate directly into a loss of business."[102] Similarly, the 2015 Makovsky Wall Street Reputation study demonstrates that 42% of U.S. consumers believe the failure to protect personal and financial information is one of the biggest threats to a financial company.[103] In the event that a breach did occur, large corporations are able to absorb the shock of the breach and damages, but a majority of the small and midsize firms are not able to maintain their businesses post-breach due to expenses of remediate measure derives from notification to every customer whose data has been compromised, public relations, damage control, risk management, among others.[104] Moreover, according to the 2013 Ponemon

---

93 *Id.*

94 *Id.*

95 David Jeffers, Don't Be the Low-Hanging Fruit, PCWorld, http://www.pcworld.com/article/257301/dont_be_the_low_hanging_fruit.html.

96 *Id.*

97 *Id.*

98 *Id.*

99 *Id.*

100 Hilary Tuttle, *Cyberbreach and Reputation Woes Hack Away at Bottom Line for 44% of Financial Firms,* RISK MGMT. MONITOR (May 29, 2015), http://www.riskmanagementmonitor.com/cyberbreach-and-reputation-woes-hack-away-at-bottom-line-for-44-of-financial-firms.

101 *See* Armerding, *supra* note 90.

102 *Id.*

103 Tuttle, *supra* note 100.

104 Kelly Phillips Erb, *Taxpayers Sue IRS For Illegal Account Access In Data Breach,* FORBES (Aug. 21, 2015), http://www.forbes.com/sites/forbesleadershipforum/2013/05/13/your-business-is-never-too-small-for-a-cyber-attack-heres-how-to-protect-yourself.

Institute research report, businesses spend almost $200 for each record that is compromised in remediation measures.[105]

The loss of customers post breach is demonstrated in the Target Breach in 2012.[106] Specifically, as statistics indicate that Generation X shoppers, from ages 32 to 49, declined from 53% to 38%, following the breach that occurred at this company.[107] In 2012, the net earnings fell from $961 million to $520 million, nearly a 46% drop.[108] Unfortunately, this was not Target's first breach. In 2013, Target experienced a second breach that resulted in 40 million credit and debit card data being compromised upon preliminary investigation.[109] Shortly thereafter, Target learned this breach was caused by third party access to the Target Point of Sale ("POS") systems.[110] This investigation focused on Fazio Mechanical Services, who had access to the POS network.[111] The hacker leveraged access using Fazio credentials, and succeeded to upload malware on the POS system undetected.[112] Following the breach, the Target CEO immediately notified customers, explaining the problem and the services Target will offer to them as compensation, such as free credit monitoring services.[113] As a result of this breach, Target also encountered multiple lawsuits from the victims of this cyber breach.[114] In March 2015, a federal judge preliminarily approved a $10 million class action settlement brought by Target customers.[115] According to the documents filed in United State District Court in Minnesota, customers affected by this breach can be award up to $10,000 per person.[116]

IV. GOVERNMENT REGULATIONS

There are more than 50 statutes that address different aspects of cyber security.[117] Yet, there is no stand-alone cyber security policy in legislation regarding the level of care

---

105 ProTechnologies, *supra* note 61.

106 Hadley Malcolm, *Target sees drop in customer visits after breach,* USA TODAY (Mar. 11, 2014), http://www.usatoday.com/story/money/business/2014/03/11/target-customer-traffic/6262059.

107 *Id.*

108 *Id.*

109 Target: 40 million credit cards compromised, CNN (Dec. 19, 2013), http://money.cnn.com/2013/12/18/news/companies/target-credit-card.

110 Jaikumar Vijayan, Target breach happened because of a basic network segmentation error, COMPUTER WORLD (Feb. 6, 2014), http://www.computerworld.com/article/2487425/cybercrime-hacking/target-breach-happened-because-of-a-basic-network-segmentation-error.html.

111 *Id.*

112 *Id.*

113 Letter from Gregg Steinhafel, Target CEO, to Target Customers Customer (Dec. 20, 2013), https://corporate.target.com/article/2013/12/important-notice-unauthorized-access-to-payment-ca (The notification letter from Gregg Steinhafel, informed the customers of the matter and urged them to remain vigilant by monitoring their billing statements and credit reports. They hired a third-party forensic firm to conduct a thorough investigation, alerted the federal authorities and financial institutions, and offered free credit monitoring and identity theft protection.).

114 Hiroko Tabuchi, *$10 Million Settlement in Target Data Breach Gets Preliminary Approval*, N.Y. TIMES (Mar. 19, 2015), http://www.nytimes.com/2015/03/20/business/target-settlement-on-data-breach.html?_r=0.

115 *Id.*

116 *Id.*

117 Fischer, *supra* note 27.

each business should implement in protecting the privacy of consumers.[118] The section below will highlight some of the most implemented regulations in practice today in various industries, such as financial institutions, health organizations, and business entities. However, the regulations in place do not discuss the standards and requirements of the small business entities prior the occurrence of the breach. Thereafter, the paper will further discuss proposed legislations and the progress made in the legislature thus far.

A. Currently Enforced Privacy Regulations

Gramm-Leach Bliley Act ("GLBA")

Due to the transition to a digital generation, and the potential privacy violations that may result from it, the government imposed the Gramm-Leach Bliley Act ("GLBA"), also known as the Financial Services Modernization Act of 1999.[119] Federal banking regulators released guidance in March 2005, establishing standards the financial institutions must comply with in order to safeguard customer's PII.[120] Analogously, section 501(b) of the Gramm-Leach-Bliley Act sets forth standards specifically for financial institutions to comply with.[121] This is set forth by various agencies such as the Federal Deposit Insurance Corporation, Office of the Comptroller of the Currency, Office of Thrift Supervision, and the Board of Governors of the Federal Reserve System.[122]

The guidance requires banks to maintain a security breach response plan, and to provide notifications to affected customers when a breach occurs.[123] The breach response plan should be in place prior to the occurrence of the breach. Since a breach, is more likely than not, to occur in any business regardless of size, the board and the staff of these businesses should know immediately how to react the moment the breach is triggered.[124] Hence, the plan should designate specific people to implement tasks, such as: recording the date and time of when the breach was discovered, alert and notify people in the company, secure the premise, prevent additional data loss, document everything known thus far about the breach, interview those who were involved, review the protocols, assess the priorities and risks, and bring in a forensic firm to further investigate the matter, and contacting the regulators.[125] Moreover, the people who are delegated responsibilities pursuant to the policy should be familiar with their role and whom they need to contact as soon as they discover the breach. Given these points,

---

118 *See generally id.*

119 The Gramm-Leach-Bliley Act, EPIC, https://epic.org/privacy/glba.

120 AMERICAN BANKERS ASSOCIATION, *Data Security & Customer Notification Requirements for Banks,* http://www.aba.com/Tools/Function/Technology/Pages/datasecuritynotification.aspx.

121 Greenberg Traurig, *Data Privacy and Gramm-Leach-Bliley Act Section 501(b),* Enterprise Risk Management (Oct. 2007), http://www.emrisk.com/sites/default/files/presentations/Data_Privacy_and_Gramm_Leach_Bliley_Act_Section_501b.pdf.

122 *Id.*

123 *Id.*

124 Micheal Whitcomb, Incident Response Success; how fast you react matters!, LORICCA (Feb. 6, 2015), http://loricca.com/incident-response.

125 Data Breach Response Guide, Experian, https://www.experian.com/assets/data-breach/brochures/response-guide.pdf.

companies need to act at a fast pace to mitigate damages and prevent further data loss to these hackers.

Financial institutions are regulated at a higher standard due to the sensitivity of the data in their record.[126] Financial institutions must ensure third-party service providers or vendors take reasonable care to comply with the objectives of the guidance and comply with section 501(b) of the GLBA.[127] Corporations are reliant upon their vendors for specialties that their corporation does not practice.[128] Steve Bridges, Senior Vice President at JLT Specialty, states "The demand for constant online communication creates enormous opportunities for hackers to exploit weak vendor security practices as a point of entry into their ultimate target."[129] According to a New York Department of Financial Services (the "NYDFS") report, nearly one-third of the 40 banks surveyed do not require the vendors to notify them of a security breach.[130] In addition, 1 in 5 banks do not require the vendors to represent that they have put in place minimum security-defense requirements.[131] Those institutions that fail to require proper representation from their vendors in regards to implementing security-defense requirements lack the direct oversight of those vendors. Further, only less than half of those institutions surveyed practice due diligence to conduct assessment of the third party vendors to ensure their security defense is on par.[132]

For years, regulators such as the Consumer Financial Protection Bureau ("CFPB") have imposed guidelines on vendor risk management and exercising due diligence to ensure that their vendors understand and are capable of complying with Consumer Financial laws.[133] Vendors are likely to put organizations at risk of reputational impact, regulatory exposure, and revenue loss, if the organization lacks the systematic approach to properly screen and assess the amount and type of access they have on sensitive customer information.[134] An IT Security Risk Survey, conducted by Kaspersky Lab, showed that the average economic impact of a single security breach was approximately $720,000 in damages.[135] If cyber-attack succeeded, it could cost the company upwards of $2.54 million.[136]

---

[126] Data Security Compliance for Financial Institutions, BLACK STRATUS, http://www.blackstratus.com/enterprise/industries/financial.

[127] AMERICAN BANKERS ASSOCIATION, *supra* note 120 (Section 501(b) outlines the privacy obligation policy to ensure the protection of nonpublic personal information.).

[128] Paul Martyn, Risky Business: Cybersecurity and Supply Chain Management, FORBES (June 23, 2015), http://www.forbes.com/sites/paulmartyn/2015/06/23/risky-business-cyber-security-and-supply-chain-management.

[129] *Id.* (JLT specialty specializes in insurance broking and risk management in cyber security, among others.).

[130] NEW YORK STATE DEPARTMENT OF FINANCIAL SERVICES, Update on Cyber Security in the Banking Sector: Third Party Service Providers, (April 2015) http://www.dfs.ny.gov/reportpub/dfs_rpt_tpvendor_042015.pdf.

[131] Greg Dickinson, Cybersecurity: Don't Bank On It With 3rd Parties, Dark Reading (Apr. 24, 2015), http://www.darkreading.com/vulnerabilities---threats/cybersecurity-dont-bank-on-it-with-3rd-parties/a/d-id/1320132.

[132] *Id.*

[133] CONSUMER FINANCIAL PROTECTION BUREAU, CFPB Bulletin (Apr. 13, 2012) http://files.consumerfinance.gov/f/201204_cfpb_bulletin_service-providers.pdf.

[134] Dickinson, *supra* note 131.

[135] Kaspersky Lab, IT Security Risks Survey 2014: A Business Approach to Managing Data Security Threats, http://media.kaspersky.com/en/IT_Security_Risks_Survey_2014_Global_report.pdf.

[136] *Id.*

The Health Insurance Portability and Accountability Act of 1996 ("HIPAA")

HIPAA was enacted by Congress to prevent the disclosure of confidential medical information and records to protect the privacy rights of individuals.[137] As a result, the medical institutions are only permitted to disclose health information if it's a necessity for patient care.[138] The act provides a series of administrative, and technical safeguards to guide the entities to assure "confidentiality, integrity, and availability of electronic protected health information."[139] Similar to business organizations, health institutions also hold a multitude of valuable and sensitive patient information that cyber criminals are after. Regardless of the size of the organization, none are immune from data breach.[140] Health organizations including hospitals, clinics, and public and private health care providers, are more vulnerable to cyber-attacks because budgets and resources, such as security expert personnel are limited compared to corporations.[141] Nonetheless, it remains a concern that cyber hackers are the number-one cause of data breach according to the Ponemon Study.[142] The study further shows that these breaches cost health care industries $6 billion annually; with the average economic impact of data breach being about $2.13 million per organization.[143]

Federal Trade Commission Act

The Federal Trade Commission Act ("FTCA") was established for the protection of the consumers from anticompetitive, deceptive, or unfair business practices.[144] The Federal Trade Commission ("FTC") was created on September 26, 1914, when President Woodrow Wilson signed the Federal Trade Commission Act into law.[145] The FTC's mission is to protect sensitive consumer information from data breaches, and to regulate cyber security.[146] The FTC's enforcement authority to prosecute for cyber security breaches derives mainly from the FTCA. Since 2002, FTC has conducted numerous investigations under Section (5) of the FTCA against companies for failures to comply with the privacy policies or engage in reasonable data security practices.[147] Section (5) of the act "prohibits unfair or deceptive acts or practices in or affecting commerce."[148] Section (5) further authorizes the examiners to

---

[137] HIPPA - Guidance Materials for Consumers, U.S. DEPT. OF HEALTH AND HUMAN SERVICES, http://www.hhs.gov/ocr/privacy/hipaa/understanding/consumers/index.html.

[138] *Id.*

[139] *Understanding Health Information Policy*, U.S. DEPT. OF HEALTH AND HUMAN SERVICES, http://www.hhs.gov/ocr/privacy/hipaa/understanding.

[140] Ponemon Institute, Criminal Attacks Are Now Leading Cause of Data Breach in Healthcare, According to New Ponemon Study (May 7, 2015), http://www.ponemon.org/news-2/66.

[141] *Id.*

[142] *Id.*

[143] *Id.*

[144] Gina Stevens, *The Federal trade Commission's Regulation of Data Security Under Its Unfair or Deceptive Acts or Practice (UDAP) Authority*, CONGRESSIONAL RESEARCH SERVICE, http://fas.org/sgp/crs/misc/R43723.pdf.

[145] FEDERAL TRADE COMMISSION, *Our History*, https://www.ftc.gov/about-ftc/our-history.

[146] *Id.*

[147] *Id.*

[148] Federal Trade Commission Act Section 5: Unfair or Deceptive Acts or Practices, http://www.federalreserve.gov/boarddocs/supmanual/cch/ftca.pdf.

regulate data security breaches as unfair trade practices.[149] By categorizing security breaches as unfair trade practice, the FTC has the authority to regulate the violation; otherwise their power to regulate the cyber breaches may be stripped from their authority.[150] The FTC believes data security vulnerabilities result from the failure to exercise due diligence.[151] Their failure to do so is considered "unfair" to consumers who entrusted their private information to the organizations.[152]

The legal standards for "unfair" acts or practices are different from those of "deceptive" acts or practices.[153] An act or practice is unfair when "it causes or is likely to cause substantial injury to consumers; cannot be reasonably avoided by consumers; and is not outweighed by countervailing benefits to consumers or to competition."[154] While, deceptive acts or practices occur where "A representation, omission, or practice misleads or is likely to mislead the consumer; a consumer's interpretation of the representation, omission, or practice is considered reasonable under the circumstances; and the misleading representation, omission, or practice is material."[155] Up until 2014, the FTC invoked the deception prong of the FTCA to bring enforcement action on almost all cyber security civil suits.[156] More recently however, the FTC have used the "unfair" prong to challenge the acts of corporations in dealing with cyber security claims.[157] Through these enforcement actions under the unfair prong, the FTC has set forth minimum requirements for companies that collect non-public personal information, even without any false representation by the company.[158] This sets a higher standard for corporations to practice greater vigilance because of their role in possessing sensitive customer information.[159] The objective of the examination is to determine whether the bank's internal procedures, policies, and controls are adequate to ensure consistent compliance with the act.[160] Through case law, federal judges have supported the FTC's position that it "possesses jurisdiction to regulate data security practices under its authority to bring enforcement actions against unfair or deceptive practices."[161]

---

149 Stevens, *supra* note 144.

150 *See generally,* Jonathan Stempel, *FTC has Power to Police Cyber Security - U.S. Appeals Court*, REUTERS (Aug. 24, 2015), http://www.reuters.com/article/wyndham-ftc-cybersecurity-idUSL1N10Z1D020150824.

151 Kevin LaCroix, Guest Post: Cybersecurity Enforcement: The FTC is Out There, The D&O Diary (Apr. 21, 2015), http://www.dandodiary.com/2015/04/articles/cyber-liability/guest-post-cybersecurity-enforcement-the-ftc-is-out-there (The company's failure to set up a robust login protocol, protect against foreseeable attacks form cyber criminals, encrypt data, and provide cybersecurity training to their employees, among others, are considered unfair to the consumers.).

152 *Id.*

153 Federal Trade Commission Act Section 5, *supra* note 148.

154 *Id.*

155 *Id.*

156 LaCroix, *supra* note 151.

157 *Id.*

158 *Id.*

159 *Id.*

160 Federal Trade Commission Act Section 5, *supra* note 148.

161 Stevens, *supra* note 144.

B. Proposed Cyber Security Regulations

Cyber criminals launched countless attacks in 2014. As a result, many corporations became victims of cyber security attacks.[162] To fight back to those cyber criminals that left millions of customers vulnerable to identity thief and fraud, governments have proposed various cyber security bills in order to regulate the field. On October 27, 2015, the Senate passed the Cyber Security Information Sharing Act.[163] This bill was designed to encourage private companies and businesses to share information about cyber security threats with the government.[164] Section 4 of the bill "[a]llows entities to share and receive indicators and defensive measures with other entities or the federal government."[165] Nonetheless, the recipients of such an indicator or defensive measure from another entity "shall comply with otherwise lawful restrictions placed on the sharing or use of such cyber threat indicator or defensive measure by the sharing entity."[166] This bill, however, has raised many controversies regarding the initiative to share customer's private information with the government, as well as other entities.[167] Industry groups, as well as an increasing number of technology companies, have argued the sharing of information would only distribute American's personal information without strengthening cyber defense and mitigating cyber threats, thus rendering the bill useless to its intended effects of protecting consumer PII.[168]

V. CYBER SECURITY CASES

One of the worst fears that corporations have after they have learned of the cyber breach is the never-ending lawsuits that will follow. The cases discussed below aim to resolve the issue of whether the plaintiffs have standing, or whether they have satisfied the requirements to bring their case to court. Different state laws define standing differently.[169] Generally for a plaintiff to have standing they need to have sustained a direct injury or harm.[170] Furthermore, this harm is redressable.[171]

---

[162] Tobias, *supra* note 89 (Millions of customer data were stolen from large corporations such as Target, Home Depot, Staples, Neiman Marcus, and Sony, who dominated the cyber breach news towards the end of 2014.).

[163] Cybersecurity Information Sharing Act of 2015, S. 754, 114th Cong. (2015).

[164] *Id.*

[165] *Id.* ("No later than 60 days after the enactment of this Act, the Attorney General and the Secretary of the Homeland Security will provide a guideline for private entities highlighting the relevant information considered to be indicators or defense measures.").

[166] *Id.*

[167] *Id.*

[168] Cory Bennett, *Controversial Cyber Bill Clears First Senate Hurdle*, THE HILL (Oct. 22, 2015), http://thehill.com/policy/cybersecurity/257720-controversial-cyber-bill-clears-first-senate-hurdle.

[169] LEGAL INFORMATION INSTITUTE, *Legal Definition of Standing*, https://www.law.cornell.edu/wex/standing.

[170] *Id.*

[171] *Id.*

A. Clapper v. Amnesty International USA

A group, which included journalists, human rights activists, and labor leaders, challenged a provision of the Foreign Intelligence Surveillance Act ("FISA").[172] The group argued that the procedure violated their fourth amendment rights. [173] The plaintiff further argued the amendments of the provision broadened the surveillance powers of the federal government. [174] This broadening of powers discouraged the groups from open communication that is essential due to the nature of their job.[175] Additionally, this provision creates a new procedure for authorizing government electronic surveillance of a person outside of the United States for foreign intelligence purposes.[176] The new provision would also force these groups to take costly measures to ensure the confidentiality of their international communications.[177] The U.S. Court of Appeals for the 2nd circuit reversed a lower court decision, holding that the groups had standing based on reasonable fear of injury and costs incurred to avoid that injury.[178]

Under the standing doctrine, in order to proceed in court, "the plaintiff must allege [a] personal injury fairly traceable to the defendant's allegedly unlawful conduct and likely to be redressed by the requested relief."[179] The Supreme Court reversed the decision of the 2nd Circuit and held that the plaintiffs lacked standing to challenge FISA because they could not know that future injury was "certainly impending", nor could they show that future injury or present costs were fairly traceable to the FISA provision. The court left the "certainly impending" standard unclear. Despite this, they did agree it should be applied to litigants challenging government action in foreign affairs or national security. Overall, *Clapper* is the first Supreme Court opinion to address the standing doctrine and reiterated that future harms are not justiciable unless injury is certainly impending and the mere allegation of a possible future injury is not sufficient.[180]

B. Remijas v. Neiman Marcus Group, LLC

The 7th Circuit Court in *Remijas* held "injuries associated with resolving fraudulent charges and protecting oneself against future identity theft" were sufficient to confer Article III standing requirement of sustaining injury.[181] This holding removed a substantial hurdle for

---

172 Clapper v. Amnesty International USA, 133 S. Ct. 1138 (2013).

173 *Id.*

174 Mark S. Melodia, and Paul Bond, *In Clapper v. Amnesty International, Supreme Court Dismisses Privacy Suit for Lack of Article III Standing: Poses a Clear and Present Danger to Data Breach Class Actions,* REED SMITH, (Mar. 1, 2013), http://www.reedsmith.com/In-Clapper-v-Amnesty-International-Supreme-Court-Dismisses-Privacy-Suit-for-Lack-of-Article-III-Standing--Poses-a-Clear-and-Present-Danger-to-Data-Breach-Class-Actions-03-01-2013.

175 *Id.*

176 Clapper v. Amnesty International USA, Oyez, https://www.oyez.org/cases/2012/11-1025 (last visited Jan. 9, 2017).

177 *Id.*

178 *Id.*

179 Allen v. Wright, 468 U.S. 737, 751 (1984).

180 Melodia, *supra* note 174.

181 Remijas v. Neiman Marcus Group, LLC, 2015 U.S.App. LEXIS 12487 (7th Cir. July 20, 2015).

data breach class actions. Earlier in *Clapper*, the Supreme Court held that future harm resulting from the data breach were not "certainly impending", thus the plaintiffs lacked the element of injury to satisfy the standing requirement.[182] *Remijas* overruled the reasoning in *Clapper,* and held that victims of a cyber breach have a reasonable expectation for what information has been compromised and what costs they will incur as a result of the breach, such as the actions taken to protect your information.[183] Plaintiffs are no longer claiming a "mere allegation of future harm", thus the 7th circuit court held that the harm is less speculative.[184] Accordingly, plaintiffs do have standing (the ability to receive relief from court.)[185]

VI. CYBER SECURITY AND INTERNATIONAL IMPLICATIONS

The May 2015 cyber breach by the IRS,[186] as discussed earlier in this note, was linked to Russia efforts to hack into the IRS system.[187] It was disclosed that Russian hackers had infiltrated both the White House and State Department computer systems, but whether it was connected to the Russia government has remain unknown.[188] The United States is well aware of the fact that foreign countries such as Russia and China have attacked U.S. commercial corporations and several U.S. officials.[189] As a result, the Obama administration was considering sanctions against both individuals and companies from Russia and China for cyber-attacks on U.S. companies.[190] China denied U.S. accusations of Chinese government supporting cyber-attacks on U.S. corporations and government officials.[191] Chinese Embassy spokesman, Zhu Haiquan, proposes to enhance dialogue and cooperation with the United States to resolve the suspicion and distrust between the countries regarding the matter of cyber breach, as oppose to baseless accusations.[192] The Embassy of Russia failed to respond to the questions from Reuter regarding the matter.[193]

In February 2015, a group of hackers targeted Anthem Inc., an American health insurance company.[194] The forensic investigation showed that the hackers were from China, but it was uncertain if the Chinese government supported them.[195] In January 2015, Anthem announced that their security system was breached and the hacker may have access to the

---

182 Melodia, *supra* note 174.

183 Jeff John Roberts, *This Court ruling just made it easier to sue companies that get hacked*, FORTUNE (Jul. 29, 2015), http://fortune.com/2015/07/29/data-breach-7th-circuit.

184 *Id.*

185 *Id.*

186 McCoy, *supra* note 75.

187 Chris Frates, *IRS believes massive data theft originated in Russia,* CNN (June 4, 2015), http://www.cnn.com/2015/05/27/politics/irs-cyber-breach-russia.

188 *Id.*

189 *US weighs sanctioning Russia as well as China in cyberattacks*, CNBC (Sept. 1, 2015), http://www.cnbc.com/2015/09/01/us-weighs-sanctioning-russia-as-well-as-china-in-cyberattacks.html.

190 *Id.*

191 *Id.*

192 *Id.*

193 *Id.*

194 Amanda Schupak, *China suspected in possible hack on America Airlines*, CBS NEWS (Aug. 7, 2015), http://www.cbsnews.com/news/china-suspected-in-hack-on-american-airlines-sabre.

195 *Id.*

private information of over 80 million Americans.[196] During that same time, the U.S. Office of Personnel Management was hacked.[197] An investigation report suggests this attack is from the same group of hackers.[198] Data such as theft of security clearance record and employee's PII were compromised.[199] Shortly thereafter in May 2015, the same hackers who had stolen data from Anthem and U.S. Office of Personnel Management were suspected to have breached another large corporation, United Airlines.[200] As a result, the hackers had access to flight details such as arrival time, departure time, seat number, as well as United Airlines' corporate details such as mergers and acquisition strategies and plans.[201] Hackers' access to the Airline's data has raised concerns of schedule disruption or transportation gridlock.[202] Any action, intentional or otherwise, may bring down sensitive systems that will affect millions of passengers annually on an international level.[203]

The thought of state-sponsored hackers obtaining access to unlimited classified information poses serious concerns for the government. In September 2015, the powerful world leaders of the U.S. and China come together to reach the China-US Cybersecurity Agreement to curb cyber security and cyber espionage between their countries (hereinafter, the "Agreement").[204] China's president Xi Jinping agrees, "Confrontation and friction are not the right choice for both sides".[205] However, within three weeks of signing the Agreement, hackers linked back to the Chinese government infiltrated American companies.[206] The companies that were hacked were from the technology or pharmaceutical firms, rather than national security related intelligence, which the Agreement does not prohibit.[207] Lawmakers expressed their concern the Agreement may be rendered useless if there is no enforcement mechanism to prevent future harms form occurring.[208]

VII. SOLUTIONS

Lawmakers believe that agreements between foreign countries to stop cyber breach are helpful, however, without a clear mechanism to enforce the agreement, cyber-attacks will

---

196 Michael Hiltzik, *Anthem is Warning Consumers About its Huge Data Breach. Here's a Translation*, LOS ANGELES TIMES (Jan. 30, 2015), http://www.latimes.com/business/hiltzik/la-fi-mh-anthem-is-warning-consumers-20150306-column.html.

197 *Id.*

198 Michael Riley & Jordan Robertson, *China-Tied Hackers That Hit U.S. Said to Breach United Airlines*, BLOOMBERG BUSINESS (July 20, 2015), http://www.bloomberg.com/news/articles/2015-07-29/china-tied-hackers-that-hit-u-s-said-to-breach-united-airlines.

199 *Id.*

200 *Id.*

201 *Id.*

202 *Id.*

203 *Id.*

204 *See* Welsh, *supra* note 22.

205 *See id.*

206 Katie Bo Williams, *China suspected of hacks after inking deal with US*, THE HILL (Oct. 19, 2015), http://thehill.com/policy/cybersecurity/257284-beijing-backed-hackers-still-hitting-us-firms-despite-agreement-report.

207 *Id.*

208 *Id.*

continue to occur.[209] Therefore, the government needs to address this concern and use this issue as a target to find an enforcement mechanism to mitigate cyber-attacks on an international level. Similar to the lack of government involvement in regulating small businesses, the requirements of commercial businesses should be enhanced by the respective government entities. The Agreement with China is a progressive step to resolving this national problem, but having the Agreement is simply insufficient. Government agencies that regulate their specific industry need to step into the commercial businesses and perform regular examinations on the business entities. If both the government and the business owners perform their respective due diligence, then the frequency of cyber-attacks would be minimized. Businesses need to be aware of the consequences and understand that proprietary and highly sensitive materials are at their hands. As demonstrated in prior cyber-attack experiences from the corporations, it can not only lead to a great loss, which would end the fate of their company, but also put consumer's privacy at risk.

Technological innovations have transformed the way people interact, communicate, share information, and do business with each other. As people become more dependent on computers for storage of mass information, replacing the traditional paper records, cyber security is recognized as one of the biggest threats faces by individuals, private and public entities. Businesses with 500 employees or smaller, designated as small businesses, making up 99.7% of our nation's business are at a greater risk.[210] Ignorance in this case is not bliss. Small businesses need to accept the fact that they are far more attractive targets than the larger corporations that generally have departments and expert personnel in place to deal with and solve problems of this category.[211] Whereas small businesses lack the necessary resources and budget to be allocated to solving a problem that has not occurred. It's time for a change in the oversight and accountability of small businesses on the issue of cyber security.

Government agencies, such as the CFPB, releases guidelines and standards for businesses that hold customer's personal information to follow.[212] However, surveys and research show that a great percentage of small businesses neglect to comply with those guidelines. Moreover, it is shown that some businesses do not exercise the most basic cyber defense protocol (i.e., to set password standards, and backing up your data.)[213] Cyber communications and transactions have become common in individuals and businesses, as such; cyber security should not be an option. It should be a requirement that every business practices. Being prepared prior to the cyber breach greatly mitigates the risk that businesses face when dealing with cyber criminals. Every business entity should submit a cyber breach response plan and represent that they will be in compliance with their own plans, in anticipation of the cyber breach. Free resources can be easily located online and accessible to anyone with Internet access.[214]

---

209 *Id.*

210 *See* SMALL BUSINESS & ENTREPRENEURSHIP COUNCIL, *supra* note 43.

211 Armerding, *supra* note 90.

212 CONSUMER FINANCIAL PROTECTION BUREAU, *supra* note 133.

213 *See* TWC Press Release, *supra* note 46 (stating that 26% of small business owners have a tough time dealing with securely backing up their data).

214 Ngoriel, 9 Cyber Security Tips for Small Business Owners, U.S. SMALL BUSINESS ADMINISTRATION (Oct. 17, 2013), https://www.sba.gov/blogs/9-cyber-security-tips-small-business-owners; *see also* A Nine-Step Guide for Smaller Merchants, ELECTRONIC TRANSACTIONS ASSOCIATION, http://www.electran.org/wp-

A. Implementing Fundamental and Mandatory Practices

Experts in the field have recommended fundamental practices that business owners must utilize. These same recommendations have been listed repeatedly in numerous cyber security firms' websites.[215] Since employees have the access to the vast majority of the client's information, cyber security experts recommend that they are up to date with protocols and preventative measures.[216] The employers need to maintain regular discussion with their employees regarding the importance of remaining vigilant.[217] Establish cyber security rules for employees on how to handle sensitive and non-public information.[218] If business resources permit, employers should consider designating a person to manage and oversee matters relating to cyber security.[219] Furthermore, employers should limit employee access and authority to download and upload software to minimize risk of downloading a virus. Employees should have access to the specific documents and software that are relevant to their department or line of work. Their authority to access software unrelated to their role should be prohibited unless provided with permission to access by their supervisor.

Since this is a cyber issue, it's essential that computers be well protected, both physically and virtually.[220] Company policy should require employees to change their login passwords frequently and regularly (i.e., once a month). Additionally employers should have a technician install and update anti-virus software to fight off spyware, and other malicious codes.[221] The anti-virus software is essentially one of the first barriers to prevent cyber criminals from attacking the network system.[222] Employers should also secure Wi-Fi network systems and make sure they are secure and hidden from unauthorized users.[223] Additionally, important data such as word documents, financial spread sheets, and client portfolios should be backed up on a weekly basis.[224]

After learning of the cyber breach, businesses should know who to contact and notify. They should have a potential forensic investigator[225] to thoroughly analyze the source of the problem, the data that was breached, and the severity of the issue. Businesses should

---

content/uploads/ETA_DataBreach_contact_2.pdf; See also Cyber Planner, FEDERAL COMMUNICATIONS COMMISSION, https://www.fcc.gov/cyberplanner.

215 *See generally,* NORTON BY SYMANTEC, *Prevention Tips,* http://us.norton.com/cybercrime-prevention; KROLL, *Data Breach Prevention Tips,* http://www.kroll.com/en-us/cyber-security/data-breach-prevention/cyber-risk-assessments/data-breach-prevention-tips; CENTRAL INSURANCE COMPANIES, *Ten Ways You Can Help Prevent a Data Breach,* http://www.central-insurance.com/docs/tips-DataBreach.htm.

216 Dan Lohrmann, What to Do About Phishing?, Government Technology (Aug. 30, 2015), http://www.govtech.com/blogs/lohrmann-on-cybersecurity/What-To-Do-About-Phishing.html.

217 *Id.* (Alert the employees to avoid downloading unauthorized documents sent be unrecognized users to prevent being the victim of cyber criminal's phishing expedition to attack and steal sensitive information.).

218 Ngoriel, *supra* note 214.

219 ELECTRONIC TRANSACTIONS ASSOCIATION, *supra* note 214.

220 CENTRAL INSURANCE COMPANIES, *supra* note 215.

221 Ngoriel, *supra* note 214.

222 Natasha Devotta, *5 Simple Steps to Protect Your PC form Hackers,* COMODO ANTIVIRUS (July 31, 2014), https://antivirus.comodo.com/blog/computer-safety/5-simple-steps-protect-pc.

223 Ngoriel, *supra* note 214.

224 *Id.*

225 What Does A Forensics Expert Do?, Cyber Degrees, http://www.cyberdegrees.org/jobs/computer-forensics (last visited Jan. 9, 2017).

know which government agency to contact pursuant to their state notifications laws.[226] Employers should also have insurance that covers cyber security breach to compensate for the damages if the breach was to occur and notify them accordingly.[227] By creating a guide of the people you must notify, you will be better prepared to deal with the post-breach chaos, and to avoid certain legal ramifications by notifying the regulators in a timely matter.

VIII. CONCLUSION

Cyber criminals often use small businesses, serving as vendors for larger businesses, as a bridge to gain access and steal data.[228] Over the past two years, more corporations are being attacked and millions of customers have become more vulnerable to the cyber criminals who have access to this data and use it to their advantage. As small businesses make up 99.7% of the nation's enterprise, regulators should make certain protocols necessary and mandatory for businesses to follow.[229] Instead of proposing guidelines for small businesses to follow, governments need to recognize that the accumulation of small businesses hold a large amount of sensitive consumer information and thus should be regulated in commensurate to the risks that it poses in the event of a cyber breach. Although posting informative suggestions of the practices that small businesses should uphold, governments need to assure that those businesses are in fact in compliance with those suggestions. Implementing the most fundamental practices such as imposing a password requirement and making the business employees aware of the importance of back up their data frequently can make crucial differences in mitigating risks. A Survey conducted by SplashData, shows that the most commonly used passwords in 2015 was "123456" and "password".[230] The government needs to make sure businesses make these fundamental requirements a mandatory business practice.

This has a tremendous impact on our economy as the foreseeable consequences such as job loss and discourage consumers from shopping and spending in fear of having their personal data being stolen. Cyber regulation of small businesses should be more than just a guideline and option for business in the age of technological innovations. The solutions proposed in this paper include minimum requirements for business that utilize computer systems and possess private information of their customers. The customers place tremendous trust on the business by believing when they swipe their credit or debit cards, they won't have to deal with security or identity fraud issues. Businesses have a standard of expectation in exercising their level of diligence to protect PII and prevent it from being in the hands of criminals, whether intentionally or unintentionally.

---

226 *See* NATIONAL CONFERENCE OF STATE LEGISLATURES, *supra* note 51.

227 ELECTRONIC TRANSACTIONS ASSOCIATION, *supra* note 214.

228 Ngoriel, *supra* note 214.

229 *See* SMALL BUSINESS & ENTREPRENEURSHIP COUNCIL, *supra* note 43.

230 Jamie Condliffe, *The 25 Most Popular Passwords of 2015: We're All Such Idiots*, GIZMODO (Jan. 19, 2016), http://gizmodo.com/the-25-most-popular-passwords-of-2015-were-all-such-id-1753591514.