Federation of Business Disciplines Journal
Volume 6, 2018 50 - 63

DATA SECURITY: A REVIEW OF MAJOR SECURITY BREACHES BETWEEN 2014 AND 2018

Ashley A. Hall
Stephen F. Austin State University
Nacogdoches, Texas 75962
USA

Carol S. Wright
Stephen F. Austin State University
Nacogdoches, Texas 75962
USA

ABSTRACT

Security breaches have been a frequent news topic in recent years. Many companies have issued statements about data security breaches that have impacted the company itself, along with customers and vendors. This research reviews the reasons behind some of these breaches and analyzes the largest breaches from 2014 – 2018. The data shows trends in the types of breaches and types of companies impacted. In addition, recommendations for businesses and educators are provided.

Key Words: cyber security, data breaches, cyber attacks

INTRODUCTION

Compromised credit card accounts. Creation of new accounts using the social security number of an unsuspecting individual. Lost healthcare data. Voter fraud. These are just a few examples of possible repercussions due to data security breaches. With the demand for services provided by companies such as LifeLock, which exists to alert customers to potential identity threats (“LifeLock,” n.d.), it raises the question “what can be done to keep people’s data safe?”

Recent examples of data security breaches fill today’s headlines. In mid-December 2013, Target Corporation discovered that the debit and credit card information of approximately 70 million customers was compromised, as well as customer details including addresses, email addresses, and phone numbers (“Data breach FAQ,” n.d.). Denning and Denning (2016) highlighted several other recent examples, including a data breach of the U.S. Office of Personnel Management which affected 22 million federal employees, the compromise of Anthem health insurance which impacted the personal data of 79 million individuals, and the data breach on Sony Pictures Entertainment which affected more than 3,000 computers by destroying data and startup software. The Sony hack also shared films not yet released and went public with embarrassing emails from executives. According to the FBI, there are two types of companies – "those that have been hacked, and those that will be" (Mueller, 2012). The hackers can range from an individual acting alone to nation states. For example, the cyberattack against Sony Pictures Entertainment was launched by North Korea (Frizell, 2015). Jenkins, Anandarajan, and D'Ovidio (2014) stated that "in our technology- and data-driven time, a data breach for an organization is not a matter of *if*, but rather of *when*" (p. 353).

These security breaches cause serious concerns for both consumers and businesses, as data security breaches entail serious threats with large-reaching financial implications. For example, the estimated costs of the December 2013 Target data breach totaled $300 million, according to Lavasoft (2015). This figure includes payments to banks and credit card companies to settle class-action lawsuits, shareholder lawsuits, Federal Trade Commission (FTC) probes, and related network security costs (Lavasoft, 2015). When hackers breached Sony's PlayStation Network in 2011, this affected an estimated 100 million customer accounts and the company faced remediation costs of at least $171 million (Goodin, 2011). This figure does not include lawsuit related expenses. According to Goodin (2011), "the estimate includes expenses of an identity theft prevention program and promotional packages to win back customers, among other things."

Statement of the Problem

Data security is proving to be increasingly difficult to manage, as there has been an increase in both internal and external threats (Richardson, 2011; vanKessel, 2011). According to the U.S. intelligence's 2013 global threat assessment, cyber threats surpassed terrorism as the top global threat to America. With the prevalence of security breaches being a frequent news topic in recent years, this leaves one to question whether information is ever completely safe. The impacts of data breaches are far reaching and include financial repercussions, as well as the potential for identity theft of unsuspecting customers. This research reviews the reasons behind some of these breaches and provides data on a selection of the largest breaches from 2014 – 2016. In addition, suggestions concerning how instructors can teach students to become diligent protectors of their own and their company's data are provided.

LITERATURE REVIEW

Sen and Borle (2015) defined a data breach as "unauthorized access to sensitive, protected, or confidential data resulting in the compromise or potential compromise of confidentiality, integrity, and availability of the affected data. Sensitive, protected, or confidential data may include personal health information, personal identifiable information, trade secrets or intellectual property, and/or personal financial data" (p. 315). Given the increase in the amount of consumer personally identifiable information (PII) that organizations collect, there is also an increase in the risks associated with securing the data and maintaining customer privacy (Moncada, 2015). The Privacy Rights Clearinghouse (PRC) began tracking data breaches in 2005. As of October 2012, leaks occurred in 563 million records. This number may actually be higher because not all breaches may have been discovered and not all breaches are reported publicly (Wikina, 2014). According to the PRC, between 2009 and 2012 there was a 230% increase in the number of records breached, which impacted approximately 27 million people (Wikina, 2014).

Challenges to Data Security

According to the National Institute of Standards and Technology (2012), cyber security attacks are increasing in number, diversity, level of damage, and disruptiveness. The interconnectedness and pervasiveness of cyber systems pose multiple challenges in the effort to maintain data security. Key challenges to data security include the complexity of the systems, the prevalence of new technologies, and human actions (or inactions).

One challenge to maintaining data security is the complexity of cyber systems and the many lines of code, or instructions, written into a program. For example, Windows 10 uses 50 million lines of code, while Mac OS 10.4 uses 86 million lines of code, and each line of code is susceptible to a security breach (Denning & Denning, 2016). Another challenge is the dynamic state of cyber systems. According to Denning and Denning (2016), companies regularly upgrade software systems, and each modification often results in the potential for new vulnerabilities to exploit.

Software companies, in an effort to quickly bring their products to market, often limit the time spent searching for and correcting vulnerabilities. A survey of over 200 developers conducted by Prevoty (2015), a security software company, found that companies release applications when there are known bugs (79% of respondents), apps with vulnerabilities are released at least 80% of the time (nearly half of respondents), and there exists a sentiment that business pressures override security issues (more than 70% of respondents).

The prevalence of new technologies also poses new security challenges for organizations. Examples include cloud computing, Bring Your Own Device (BYOD) policies, social media, and mobile devices. In cloud computing, "company and personal data are intermingled across networks, applications, devices and storage media" (Snell, 2016, p. 22). BYOD policies that allow employees to use their own devices for work purposes also pose data security challenges. If the device is hacked, stolen, or inadvertently lost, company data is lost or at risk as well (Snell, 2016). A 2008 study conducted by the Ponemon Institute and sponsored by Absolute Software found that over 9 out of 10 (92%) IT security practitioners reported someone in their organization losing a laptop or having it stolen. In addition, 71% reported that the loss or theft of the laptop resulted in breached data.

The Human Factor

IBM (2013) found that approximately 80% of the vulnerabilities that cyber attackers exploit are human vulnerabilities. Even so, the focus of cybersecurity efforts has largely been on technology and systems tools (Hershberger, 2014). In a recent study, Unisys (2014) found that over half (54%) of the breaches in 2013 were a result of employee negligence. According to Adams and Makramalla (2015), "human vulnerabilities include, but are not limited to, employee negligence, leadership misinformation and limited cybersecurity skills training, malicious insiders, and third parties who have access to an organization's network" (p. 5).

Examples of user behaviors that make data security more challenging include utilizing weak passwords, opening attachments or clicking links haphazardly, and people who lose their portable devices or fall for a phishing scam. System administrators can also leave the network vulnerable to cyberattacks by not setting up appropriate security systems, or by failing to install patches, respond quickly to security alerts, or remove accounts that are obsolete (Denning & Denning, 2016). Responding timely is essential, yet a study of 50,000 organizations conducted by Kenna Securities found that the average length of time it takes a company to install patches is 100

– 120 days. This fact is alarming considering that the probability of exploitation of a security vulnerability is 90% in a 60-day window (Kenna Security, 2015).

Wikina (2014) discussed various types of breaches including “hacking or IT incidents, theft, loss, unauthorized access or disclosure, [and] improper disposal” (p. 3). It was acknowledged that a variety of infrastructure was impacted, including desktop and laptop computers, email systems, electronic health records, paper records, and servers (Wikina, 2014). Interestingly, Wikina (2014) found that “even with the increasing use of IT in healthcare, the vast majority of data breaches affecting individuals appear to be the result of theft and loss, not hacking or IT incidents” (p. 4).

Although employee negligence or carelessness can result in data breaches, people also play an important role in data security efforts. Hershberger (2014) noted that when the Target Corporation experienced a data breach in 2013, the security systems in place effectively detected the breach; however, the people responsible for correcting the breach did not have the requisite skills and knowledge on what to do in response. It is unfortunate that employees often lack sufficient training on what to do in such a situation. Unisys (2014) found that only 6% of companies surveyed identified offering training on cybersecurity to all employees as a top security objective.

Impacts of Data Breaches

Data breaches affect both consumers and companies. Identity theft and fraud are major concerns in the aftermath of a data security breach. While the two terms are often used interchangeably, nuanced differences do exist, and identity fraud often occurs as a result of identity theft (Consumer Info, 2015). Identity theft is the greatest impact of data breaches on individuals, and 12.7 million victims of identity fraud suffered an estimated $16 billion loss in 2014 (Pascual & Miller, 2015). One of the fastest growing white-collar crimes in the United States is identity fraud (Javelin Strategy & Research, 2015).

In June 2014, Securities and Exchange Commission (SEC) Commissioner Luis Aguilar cautioned that organizational boards should “prepare the company for the inevitable cyber attack and the resulting fallout from such an event.” The Center for Strategic and International Studies 2014 report, funded by McAfee, estimated the costs of cyber crime globally to be more than $400 billion a year (Nakashima & Peterson, 2014). According to that same report, the United States lost an estimated $100 billion in 2013 when considering both direct and indirect costs of cyber attacks.

In addition, companies must also pay to defend themselves in lawsuits that often occur as a result of data breaches. For example, Sony is incurring legal costs related to defending itself against 58 class action lawsuits filed in response to the breach, as well as any damages if the company is found liable (Perlroth, 2011). This makes data breaches very expensive for organizations.

Targeted Attacks

Sherstobitoff (2008) commented that there has been an increase in malware that is targeting specific platforms. Such tailored malware targets an organization’s intellectual property and can “remain under the radar for extended periods of time, thus going undetected by resident security software until it is too late” (Sherstobitoff, 2008, p. 248). Such attacks utilize a variety of all-too-believable tactics in an effort to encourage the victims to execute the Trojan attached to the message. Fake subpoenas or tax documents are two such examples. The author noted that “Spear phishing tactics have begun to replace generic forms of phishing as users began to recognize they were not legitimate. When targeting a company to obtain specific information, hackers will develop a phishing campaign designed for that company alone, researching and obtaining information concerning their targets to ensure the message sent is believable" (Sherstobitoff, 2008, p. 248).

Electronic health records are also prime targets for data security breaches. Data breaches impacted over 500 individuals and affected more than 29 million records between 2010 and 2013 (Liu, Musen, & Chou, 2015). The Ponemon Institute's second annual benchmark study, published in 2011, found that employee negligence was the primary reason for data breaches within healthcare organizations. However, the sixth annual study, published in 2016, found that "for the second year in a row, criminal attacks are the leading cause of data breaches in healthcare" (p. 1). Interestingly, when asked to select the three types of security threats that worry them the most, more respondents answered negligent or careless employees (69%) than cyber attacks (45%) (Ponemon, 2016).

According to the California Dental Association (2016, p. 49), "The U.S. Department of Health and Human Services' (HHS) online listing of protected health information breaches, known as the 'wall of shame,' includes nearly 1,400 incidents of major data breaches (affecting 500 or more people) since 2009 when the HIPAA Breach Notification Rule began." Eastwood (2012) posited that healthcare organizations need to be cognizant of hacking, "even though hacking accounts for just 8 percent of data breaches, because personal health information is worth 50 times more to hackers and data thieves than credit card or Social Security numbers" (Wikina, 2014, p. 3). According to Yao (2017), social security numbers sell for 10 cents and credit card numbers sell for 25 cents on the black market, but electronic health records sell for hundreds or, at times, thousands of dollars. The reason for this is that EHRs (electronic medical health record) have an abundance of personal information to exploit (Yao, 2017). Examples of information available include "names, birth dates, policy numbers, diagnosis codes and billing information" (Humer & Finkle, 2014). This information is then used to generate fake IDs to purchase medical equipment or prescription drugs which can be resold. Another example of how the purchased information could be inappropriately used is by combining a patient number with a generated provider number to file imaginary claims (Humer & Finkle, 2014). In an interview, Marc Probst, CIO of Intermountain Healthcare in Salt Lake City, commented that "The only reason to buy that data [from EHRs] is so they can fraudulently bill" (Humer & Finkle, 2014).

Data Breach Legislation and Reporting

The Federal Trade Commission (FTC) is the U.S.'s primary enforcement agency policing threats against consumer safety and data privacy (Moncada, 2015). The FTC encourages the self-regulation of businesses by suggesting the creation of company-specific security programs based on their business model (Moncada, 2015). State-specific legislation dictates required notification of security breaches. There are 48 states that require notification on the part of private or government entities when there are breaches of personally identifiable information. Alabama and South Dakota do not have security breach laws at this time ("Security Breach Notification Laws," 2017). Schneider (2009) noted that state statutes typically require businesses to acknowledge breaches publicly and to alert those affected to take precautions. While federal legislation regulating data security and notification is not in place at this time, industry-specific statutes do exist (e.g., HIPAA for healthcare, GLBA for financial services) (Fisher, 2013; Zelle & Whitehead, 2014).

THE STUDY

To study the most recent data breaches and bring the academic literature current, the authors compared lists of the most severe data breaches as reported by Forbes magazine and Identity Force, an organization that provides identity, privacy, and credit protection (Hardekopf, 2015; Identity Force, 2015; Identity Force, 2016; Ramanan, 2015; Identity Force, 2017; Identity Force, 2018). After comparing the lists and eliminating duplicates, the findings present the results from the two groups. The two lists presented information about the breaches, including companies effected, the reasons for the breach, and who was ultimately affected. The findings do not present any other data breaches from other companies in the analysis.

Table 1 below provides the list of top data breaches for 2014 - 2016. The analysis uses the following occurrences as part of this study:

Table 1
List of Companies Used for Study, Identified by Source

Forbes 2014 (Hardekopf, 2015)	**Forbes 2015** (Ramanan, 2015)	**Identity Force 2015** (Identity Force, 2015)	**Identity Force 2016** (Identity Force, 2016)
Neiman Marcus	Slack	*Anthem	FACC
White Lodging	Hacking Team	*Premera BCBS	University of Central Florida
Sally Beauty	Kaspersky	**International Banks	U.S. Dept. of Justice
Michaels	*CareFirst BCBS	Equifax	Internal Revenue Service
Affinity Gaming	LastPass	*CareFirst BCBS	U.C. Berkeley
**New York Attorney General	*Premera BCBS	Internal Revenue Service	Snapchat
PF Changs	*Experian/T-Mobile	*AdultFriendFinder.com	21 Century Oncology
Albertsons/SuperValu	*Office of Personnel Management	*Office of Personnel Management	Premier Healthcare
Community Health Systems	*Ashley Madison	Houston Astros	Verizon Enterprise Solutions
UPS	*Anthem	*Ashley Madison	Systema Software
Dairy Queen		CVS Photo	Tidewater Community College
Goodwill		UCLA Health Systems	MedStar Health
Home Depot		United Airlines	Phillipine Commission of Elections
Jimmy Johns		**iPhones	**Multiple email providers
*JP Morgan Chase		*Experian/T-Mobile	Wendy’s
Sourcebooks		Law Enforcement Enterprise Portal	LinkedIn
Kmart		Comcast	NewKirk Products
Staples		*JP Morgan Chase and others	Oracle
Bebe		Hilton Worldwide	Dropbox
Sony		Vtech Holdings	Yahoo
			Weebly
			National Payment Corporation of India
			Cisco
			*AdultFriendFinder.com
			San Francisco Municipal Transportation Agency

Using the above table as part of the study data, items designated with a single asterisk (*) are duplicates and are only counted once in data analysis. Another duplication includes JP Morgan Chase. The Forbes list identified it by itself, but the Identify Force list groups it with other financial. Because JP Morgan was the bank mentioned to have the most number of customers effected, it is counted as one company for data analysis. Items designated with a double asterisk (**) are not used in this study because they do not identify a specific organization that was targeted. These data breaches include the New York Attorney General's Office who identified multiple breaches, the international bank hacks which effected more than 100 banks, iPhone breaches that were targeting a product, and breaches that effected multiple email providers without one specific provider being the target.

Table 2 below provides the list of top data breaches for 2017 through October of 2018. The analysis uses the following occurrences as part of this study:

Table 2
List of Companies Used for Study for 2017 and 2018, Identified by Source

Identity Force 2017 (Identity Force, 2018)		**Identity Force 2018** (Identity Force, 2018)	
TalentPen & TigerSwan	Dun & Bradstreet	Bithumb	Coinrail
Uber	Maine Foster Care	GovPayNow	SunTrust Banks
University of Oklahoma	Online Spambot	Chicago Public Schools	Nashville Metro Public Health
eBay	Deep Root Analytics	Rail Europe	SSM Health St. Mary's
TIO Networks	River City Media	FedEx	Med Associates
InterContinental Hotels	Brooks Brothers	Central Maine Power	CarePlus
California Assoc. of Realtors	Kmart	Dignity Health	Reddit
DocuSign	Arby's	LifeLock	Google
E-Sports Entertainment	Xbox 360 & PSP	Exactis	MongoDB Server
UNC Health Care	America's JobLink	Sitter	Panera Bread
FAFSA – IRS	Bronx Lebanon Hospital	Independence Blue Cross	TCM Bank
Equifax	Sonic	BJC Healthcare	Various U.S. universities
Disqus	Imgur	Partners HealthCare	Jason's Deli
OneLogin	SVR Tracking	Chili's	St. Peter's Surgery & Endoscopy
Verifone	Whole Foods Market	Orbitz	Under Armour
Hyatt Hotels	Forever 21	City of Goodyear	LifeBridge Health
Sabre Hospitality Solutions	Gmail	Ticketfly	TaskRabbit
Chipotle	Washington State University	Adidas	Timehop
Saks Fifth Avenue	Deloitte	Polar Fitness Trackers	Macy's
U.S. Securities & Exchange Commission	Verizon	ComplyRight	Adams Country
		Fortnite	Animoto
		T-Mobile	Air Canada
		mSpy	British Airways
		Chegg	Apollo
		Department of Defense	U.S. Center for Medicare & Medicaid
		Cathay Pacific	Legacy Health
		Instagram	SHEIN
		Nuance Communications	Eastern Maine Community College

		Orrstown Bank	ATI Physical Therapy
		Inogen	Unity Point Health
		Aultman Health Foundation	MedSpring Urgent Care
		Augusta University	Foosackly's
		Ticketmaster	Newegg
		UMC Physicians	Boys Town National Research Hospital
		Toyota	Click2Gov
		Saks First Ave. and Lord & Taylor	Cheddar's Scratch Kitchen
		U.S. Air Force	Facebook
		University of Buffalo	LabCorp Diagnostics
		MyHeritage	Jones Eye Clinic

FINDINGS

This study includes 182 different organizations including private and public businesses, government agencies, and educational institutions. Of these reported breaches, 48 out of 182 (80.8%) effected the organizations' customers (including users of the systems and students for educational institutions). Of the remaining breaches, 7.7% effected current, future, and/or former employees, 3.8% effected the organization itself, 2.7% effected voters and/or taxpayers. Based on our data source, 8.8% of the organizations did not have a reported target of the attack at the time of the disclosure. The percentages exceed 100% because some data breaches effected multiple parties.

Data breaches appear to run in cycles as to how they occur. Whereas in 2014 data breaches seemed to mostly target in-store point-of-sale systems (POS) (79% of the time), 2015 saw an increase in hackers finding ways to penetrate secure systems to gain information (90% of the time). 2016 had online hacking as the most common occurrence (72% of the time). Although online hacks were still common, 2017 and 2018 saw a rise in the number of company errors that caused the breach. Table 3 below categorizes the types of data breaches analyzed.

Table 3
Types of Data Breaches by Year

	2014	2015	2016	2017	2018
In-store P.O.S. systems	79%	5%	4%	27%	6%
Hack of online system including malware	21%	90%	79%	32%	56%
Phishing scams – employee error	-	5%	8%	5%	9%
Other – internal error of system or employee error	-	-	4%	29%	24%
Other – physical stolen property	-	-	4%	2%	1%
Unknown/Not disclosed				5%	3%

Data breaches also appear to target certain types of businesses. In 2014, 75% of targeted institutions were retail businesses, but in 2015 only 10% of affected organizations were in retailing. Instead, 2015 saw 24% of breaches in technology companies, 19% in medical organizations, and 14% in entertainment. Similarly, 2016 brought breaches from technology (21%), medical (17%), social (8%), and government (8%) organizations. Similar trends were seen in 2017 and 2018. One interesting change in 2018 included two major hacks at cryptocurrency companies totaling a loss of over $69 million in online currency being stolen.

Regardless of year, industry, or data breach, a tremendous number of people and organizations have been affected by the abundance of data breaches in the last few years. Reports of data breaches do not always report the number of people effected by the breaches, which makes studying the topic more challenging. Yahoo! has, by far, had the largest data breach with one billion customer accounts compromised from an online hack. Yahoo! divulged two large breaches during 2016, which makes the company have the largest data breach in history. Yahoo! disclosed that every one of its user accounts were affected by the breach (Identity Force, 2017). The next five largest data breaches by the number of people effected amounts to 474 million individuals and includes data breaches of AdultFriendFinder.com (412 million), LinkedIn (117,000,000), Home Depot (109,000,000), and JP Morgan Chase and other banks (100,000,000), and Anthem (80,000,000).

DISCUSSION

Although Unisys (2014) reported 54% of the breaches in 2013 were a result of employee negligence, the largest security breaches the following three years showed that various types of security hacks were to blame. This number increased again, however, in 2017. Data breaches at retail business were predominant in 2014. They also affected the largest number of people, as shown in the breach at Home Depot, which impacted 109 million customers. Online hacks of company P.O.S. systems are still prevalent, but they seem to not be the most common occurrence now.

Following the reporting of Sherstobitoff (2008), the latest data breaches did show an increase in malware that targeted specific platforms. This was evident in the targeting of point-of-sale systems that were prevalent in 2014 and the various hacks in 2015 and 2016. What is more concerning are the types of companies targeted in 2015. As reported in the Forbes 2015 list (Ramanan, 2015), The Hacking Team, which develops spying tools for various governments, had its customer list revealed. In addition, Kaspersky, who develops anti-virus software, also had its system breached, but the hackers were reportedly trying to learn about the company's technology "to try to stay under the radar" (Kaspersky, 2015, para. 6). LastPass, a password management company that stores a master password for its customers, was also hacked.

The data does show an increase in public breaches of electronic health records, which aligns with the research presented by Liu et al. (2015). Medical organizations had the second highest number of large breaches in 2015, and at least 3.5 million people were affected by a breach of medical records in 2016 alone (Identity Force, 2016). The large data breaches at Yahoo! show a shift to the hacking of personal information at technology companies as the most common type of breach in 2016.

Implications

It is evident from the research that no company is immune from the possibility of a data breach. It seems startling that the recent data breaches appear to be more sophisticated in that the targets are often technology-based companies that one would assume would have strict security measures in place. However, it seems hackers are also becoming just as sophisticated as they are hacking the companies whose purpose is to avoid hacking (e.g., Kaspersky, LastPass, and LifeLock). Companies and consumers need to be diligent in protecting their data and prepare to take steps to minimize the effects of a breach that is likely to occur.

For a company, fast disclosure to the effected parties is important through clear communication. Vinton (2014) stressed “that transparency and communication is key, as clients are often more concerned with how an organization responds to a breach than the fact that it occurred” (para. 5). Timely, quality communication is an important business implication of this study.

Action Steps

It may be beneficial for everyone (customers, companies, and employees alike) to take the position that no system is secure. Ramanan (2015) warns that attacks will continue and will become more intense. He predicts these hacks will affect more security organizations, that there will be an increase in black market hacks, and more attacks led by nation states.

With the goal of mitigating data breaches, there are numerous action steps to teach both students and employees. While many of them may seem elementary when compared to the sophistication of today’s cyber-attacks, a few simple steps can help reduce the risk of employee negligence being the culprit behind lost data. Although there has been much discussion about steps to take to avoid data breaches, the increase in company errors in the last two years shows that training is still needed in basic data protection. Lord (2018) details steps that institute best practices when protecting data. These steps include:

- Use strong passwords – Create unique passwords using a variety of capitalization, punctuation, and numbers (Deep Root Analytical failed to put passwords on certain files).
- Keep passwords confidential – Do not share passwords with others or allow them to log in under an account that is not theirs. Do not respond to email requests to enter login credentials.
- Follow data security measures in place within the organization – Do not turn off security features on company computers, and allow software to automatically update (Deloitte did not follow two-factor authentication methods)
- Be suspicious of links and attachments – Click with caution. Avoid opening unexpected email attachments which may contain viruses (Multiple companies including Orrstown Bank, Unity Point Bank, and Augusta University experienced breaches because employees were targeted by phishing emails).
- Exercise due diligence – Do not leave portable electronic devices unattended. When leaving the physical workspace, lock the computer to prevent unauthorized access and ensure no confidential information is visible. Turn off the computer and disable wireless connections and file sharing when not in use (Nashville Metro Public Health had information stolen by an employee).

As the data shows, data breaches are becoming increasingly complex. The number of breaches because of employee negligence has decreased, and malicious attacks are increasing. The company must consistently practice due diligence to constantly monitor their systems because it seems that the criminals are becoming more sophisticated. Unfortunately, this due diligence is falling on the advanced information technology personnel in the company. Constant training is needed to stay abreast of new technologies, but little research has been available to address how often trainings are conducted or how they are instituted.

CONCLUSION

In response to the increasing amount of information stored and transmitted electronically, data security has become a pressing concern for businesses. The fallout that occurs in response to a data breach significantly impacts the business as well as the lives of the customers whose information was compromised. This study analyzed the top data breaches of 2014 through 2018, and found that a variety of attacks occurred employing different strategies, which makes data security more complex. Companies that reported these breaches are beginning to suffer additional consequences after the initial breach. For example, Blue Cross Blue Shield/Anthem, who reported a breach in 2015, settled with the FBI to offer customers additional credit monitoring services and pay a $115 million fine (Identity Force, 2017) and VTech Technologies was fined $650,000 by the FTC for its failure to require parental consent before collecting personal information from children.

Given the likelihood that organizations will fall victim to data breaches, educators and businesses have a responsibility to equip students and employees with an understanding of basic data security principles. Doing so can help protect both the individual's data, as well as the business', which will have major fiscal implications given the exorbitant costs of data breaches. Instructors should emphasize that there are a variety of ways for data to be compromised. By providing examples of recent data breaches, educators can showcase various methods being used and discuss appropriate data security strategies with students.

FUTURE RESEARCH

Future research of data breaches should continue to follow trends of data breach sources, as it seems these breaches run in cycles. Future research could also study individual companies and their training programs to understand how employees are trained to protect data and whether this training is effective.

REFERENCES

Adams, M., & Makramalla, M. (2015). Cybersecurity skills training: An attacker-centric gamified approach. *Technology Innovation Management Review, 5*(1), 5-14.

Aguilar, L. A. (2014, June 10). Boards of directors, corporate governance and cyber-risks: Sharpening the focus. Retrieved from https://www.sec.gov/News/Speech/Detail/Speech/1370542057946

California Dental Association (2016, January). Top seven data breach considerations. *CDA Journal*, *44*(1), 49-52.

Consumer Info, Inc. (2015, January 12). Identity theft and identity fraud. Retrieved from https://www.freecreditscore.com/blog/identity-theft-identity-fraud/

Data breach FAQ (n.d.). Retrieved from https://corporate.target.com/about/shopping-experience/payment-card-issue-FAQ

Denning, P. J., & Denning, D. E. (2016). Cybersecurity is harder than building bridges. *American Scientist*, *104*(3), 154-157. doi: 10.1511/2016.120.1

Eastwood, B. (2012). How to prevent healthcare data breaches (and what to do if you're a victim). *CIO.* Retrieved from http://www.cio.com/article/2389573/healthcare/how-to-prevent-healthcare-data-breaches--and-what-to-do-if-you-re-a-victim-.html

Fisher, J. A. (2013). Secure my data or pay the price: Consumer remedy for the negligent enablement of data breach. *William & Mary Business Law Review, 4*(1), 215-239.

Frizell, S. (2015, January 8). NSA director on Sony hack: 'The entire world is watching' *Time.* Retrieved from http://time.com/3660757/nsa-michael-rogers-sony-hack/

Goodin, D. (2011, May 24). PlayStation Network breach will cost Sony $171m and counting. *The Register*. Retrieved from http://www.theregister.co.uk/2011/05/24/ sony_playstation_breach_costs/

Hardekopf, B. (2015, January 13,). The big data breaches of 2014. *Forbes*. Retrieved from http://www.forbes.com/sites/moneybuilder/2015/01/13/the-big-data-breaches-of-2014/#64a3ca343a48

Hershberger, P. (2014). Security skills assessment and training: The “make or break” critical security control. *SANS Institute InfoSec Reading Room.* Retrieved from https://www.sans.org/reading-room/whitepapers/leadership/security-skills-assessment-training-critical-security-control-break-o-35637

Humer, C., & Finkle, J. (2014, September 24). Your medical record is worth more to hackers than your credit card. *Reuters*. Retrieved from http://www.reuters.com/article/us-cybersecurity-hospitals-idUSKCN0HJ21I20140924

IBM (2013). The 2013 IBM cyber security intelligence index. Retrieved from http://www-935.ibm.com/services/us/en/security/infographic/cybersecurityindex.html

Identity Force. (2015, March 27). The biggest data breaches of 2015, so far. Retrieved from https://www.identityforce.com/blog/2015-data-breaches

Identity Force. (2016, December 16). The biggest data breaches in 2016. Retrieved from https://www.identityforce.com/blog/2016-data-breaches

Identity Force. (2017, December 14). 2017 Data breaches – The worst so far. Retrieved from https://www.identityforce.com/blog/2017-data-breaches

Identity Force (2018, October 25). 2018 Data breaches – The worst so far. Retrieved from https://www.identityforce.com/blog/2018-data-breaches

Javelin Strategy & Research (2015, March). 2015 identity fraud study. Retrieved from https://www.javelinstrategy.com/press-release/16-billion-stolen-127-million-identity-fraud-victims-2014-according-javelin-strategy

Jenkins, A., Anandarajan, M., & D’Ovidio, R. (2014). “All that glitters is not gold”: The role of impression management in data breach notification. *Western Journal of Communication, 78*(3), 337-357. doi: 10.1080/10570314.2013.866686

Kaspersky, E. (2015, June 10). Kaspersky Lab investigates hacker attach on its own network. Retrieved from https://blog.kaspersky.com/kaspersky-statement-duqu-attack/8997/

Kenna Security (2015, September). How the rise in non-targeted attacks has widened the remediation gap. Retrieved from https://www.kennasecurity.com/resources/non-targeted-attacks-report/

Lavasoft (2015, December 7). Cost of Target’s holiday season data breach: $300 million. Retrieved from http://www.lavasoft.com/mylavasoft/company/blog/cost-of-target%E2%80%99s-holiday-season-data-breach-300-million

LifeLock (n.d.). Retrieved from https://www.lifelock.com/

Lord, N. (2018, January 29). 101 Data protection tips: How to keep your passwords, financial & personal information safe. *Digital Guardian*. Retrieved from https://digitalguardian.com/blog/101-data-protection-tips-how-keep-your-passwords-financial-personal-information-safe#DevicesNetworks

Liu, V., Musen, M. A., & Chou, T. (2015). Data breaches of protected health information in the United States. *JAMA, 313*(14), 1471-1473.

Moncada, A. R. (2015). When a data breach comes a-knockin', the FTC comes a-blockin': Extending the FTC's authority to cover data-security breaches. *DePaul Law Review, 64*(3), 911-944.

Mueller III, R. S. (2012, March 1). RSA cyber security conference. Retrieved from https://archives.fbi.gov/archives/news/speeches/combating-threats-in-the-cyber-world-outsmarting-terrorists-hackers-and-spies

Nakashima, E., & Peterson, A. (2014, June 9). Report: Cybercrime and espionage costs $445 billion annually. *The Washington Post*. Retrieved from https://www.washingtonpost.com/world/national-security/report-cybercrime-and-espionage-costs-445-billion-annually/2014/06/08/8995291c-ecce-11e3-9f5c-9075d5508f0a_story.html

National Institute of Standards and Technology (2012). Computer security incident handling guide. Retrieved from http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

Pascual, A., & Miller, S. (2015, March). Identity fraud report protecting vulnerable populations. *Javelin Strategy and Research.* Retrieved from http://securityaffairs.co/wordpress/34449/cyber-crime/javelin-study-2015-identity-fraud.html

Perlroth, N. (2011, December 29). Insurance against cyber attacks expected to boom. *NY Times Bits*. Retrieved from http://bits.blogs.nytimes.com/2011/12/23/insurance-against-cyber-attacks-expected-to-boom/?_r=0

Prevoty, Inc. (2015). The impact of security on application development: 2015 survey report. Retrieved from http://info.prevoty.com/impact-of-security-on-agile-development-report

Ponemon Institute, LLC (2008, December). The human factor in laptop encryption: US study. Retrieved from http://www.ponemon.org/local/upload/file/Absolute%20Software%20Final%20%20United%20States.pdf

Ponemon Institute, LLC. (2016, May). Sixth annual benchmark study on privacy & security of healthcare data. Retrieved from http://media.scmagazine.com/documents/232/sixth_annual_benchmark_study_o_57783.pdf

Ponemon Institute, LLC (2011, December). Second annual benchmark study on patient privacy & data security. Retrieved from https://clearwatercompliance.com/wp-content/uploads/2011_Ponemon_ID_Experts_Study.pdf

Ramanan, S. (2015, December 31). The top 10 security breaches of 2015. *Forbes*. Retrieved from http://www.forbes.com/sites/quora/2015/12/31/the-top-10-security-breaches-of-2015/#16b18cc4694f

Richardson, R. (2011). 2010/2011 computer crime and security survey. *Computer Security Institute.* Retrieved from http://reports.informationweek.com/abstract/21/7377/Security/research-2010-2011-csi-survey.html

Schneider, J. W. (2009). Preventing data breaches: Alternative approaches to deter negligent handling of consumer data. *Boston University Journal of Science & Technology Law, 15*(2), 279-304.

Security breach notification laws (2016). Retrieved from http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx

Sen, R., & Borle, S. (2015). Estimating the contextual risk of data breach: An empirical approach. *Journal of Management Information Systems, 32*(2), 314-341.doi: 10.1080/07421222.2015.1063315

Sherstobitoff, R. (2008). Anatomy of a data breach. *Information Security Journal: A Global Perspective, 17*, 247-252. doi: 10.1080/19393550802529734

Snell, E. (2016, May). HR and IT joining forces against cyberattacks. *Benefits Magazine, 53*(5), 20-25.

U.S. Intelligence Community (2013, March 12). Worldwide threat assessment. Retrieved from https://www.odni.gov/files/documents/Intelligence%20Reports/2013%20ATA%20SFR%20for%20SSCI%2012%20Mar%202013.pdf

Unisys (2014). Critical infrastructure: Security preparedness and maturity. Retrieved from https://www.hunton.com/files/upload/Unisys_Report_Critical_Infrastructure_Cybersecurity.pdf

vanKessel, P. (2011). Into the cloud, out of the fog: Ernst & Young's 2011 global information security survey. Retrieved from http://www.ey.com/Publication/vwLUAssets/%c5%9awiatowe_badanie_bezpieczenstwa_informacji_2011/$FILE/ey_swiatowe_badanie_bezpieczenstwa_informacji_2011_07112011.pdf

Vinton, K. (2014, July 1). How companies can rebuild trust after a security breach. *Forbes*. Retrieved from http://www.forbes.com/sites/katevinton/2014/07/01/how-companies-can-rebuild-trust-after-a-security-breach/print/

Wikina, S. B. (2014). What caused the breach? An examination of use of information technology and health data breaches. *Perspectives in Health Information Management*, 1-16.

Yao, M. (2017, April 14). Your electronic medical records could be worth $1000 to hackers. *Forbes*. Retrieved from https://www.forbes.com/sites/mariyayao/2017/04/14/your-electronic-medical-records-can-be-worth-1000-to-hackers/

Zelle, A. R., & Whitehead, S. M. (2014). Cyber liability: It's just a click away. *Journal of Insurance Regulation, 33*, 145-168.

ABOUT THE AUTHORS

Ashley A. Hall is an Assistant Professor in the Department of Business Communication & Legal Studies in the Nelson Rusche College of Business at Stephen F. Austin State University, where she teaches business communication, employee development, and records management courses. Dr. Hall received her PhD in Human Resource Development from the University of Texas at Tyler. Her scholarly publications include topics such as managerial competencies, social media and hiring practices, and pedagogical research.

Carol S. Wright is an Associate Professor in the Department of Business Communication & Legal Studies at Stephen F. Austin State University, where she teaches business communication and general business courses. Dr. Wright received her EdD in Educational Leadership from Stephen F. Austin State University. Her scholarly publications include topics in business communication, social media, and pedagogical research.