A Conceptual Solution for Consumers' Data Security Protection in the U.S. General and HealthCare Industry

Kay K. Kim

Fitchburg State University, Fitchburg MA 01420 USA

Abstract- The purpose of this paper is to define and explain the importance of cyber security and the impact cyber data breaches have on the consumer. This paper also tries to explore several different methods to help protect data while also using real-world examples of some data breaches that have occurred in recent history as well as in the US healthcare industry.

Index Terms- Networks, Data Security, Data Breach, Hacking, Remote Connectivity, Personally Identifiable Information, Data Encryption, Electronic Health Records

I. Introduction

We live in a world of ever-changing technology, which has its advantages and disadvantages as well as challenges and issues that must be addressed. When it comes to the business industry, organizations must consider a consumers' privacy and security concerns. By changing from paper to electronic business data records consumer's information is vulnerable to security breaches. It is important to have confidentiality, integrity, and available of all electronic data records. Creating a comprehensive security system is the key to avoiding data breaches and gaining a consumer's trust in your security system. To make adequate changes, the country as a whole must ban together and passes legislation that creates standards for all business organizations to follow.

For any company looking to offer flexible data accessibility options to their employees, the primary goal should always data security. Not only does this protect the company from the embarrassment and financial backlash of a data breach, but it also protects the company's clients from having their own data compromised – knowingly or unknowingly. For perspective, Target is rumored to be paying over $100 million in settlement claims to Visa and MasterCard and even more in legal fees, fines, and credit monitoring (Sidel, 2015) in the aftermath of the data breach that occurred in 2013. If a company as large and successful as Target is susceptible to a data breach, how limited are the alternatives for firms to strike a balance between data accessibility and data security?

A GALLUP poll shows that telecommuting in the US has climbed to 37% in 2015; up 7% from a decade ago (Jones, 2015). Given that more and more jobs are offering telecommuting as a benefit for employees this percentage will likely continue to increase over time. There is also an inherent benefit to companies looking to cut overhead expenses by maintaining a cyber-workforce, so-to-speak. When companies allow employees to telecommute, however, they also open themselves up to potential data breaches by hackers. Having the proper network security features in place may not fully protect a company from a breach, but it can at least act as a strong deterrent to keeping hackers at bay.

2.1 WHAT IS CYBER DATA SECURITY

Often referred to as information technology, cyber security is the act of protecting computers, networks and data from unauthorized access. [7] For years, as consumers, we have been warned of viruses penetrating our personal computers and corrupting our files and rendering our computers useless. Every aspect of business now a day, collects and stores large amount of data. Data on customers may include credit card information, mailing addresses or it could be healthcare patients' sensitive medical information. This massive collection of information is not just stored on networks but oftentimes are transmitted over the web, shared with other entities. As Government, businesses, healthcare systems and families collect, store, process and transmit all this data, the data could become vulnerable to access by unwanted persons. In a March 2013 Senate session, a warning from the Nation's top intelligence officials claimed cyber-attacks and digital spying are the top threat to national security, surpassing terrorism. [7]

2.2 TYPES OF CYBER DATA ATTACKS

There are several types of data breaches. This section will give examples of the most common and most dangerous types and define each one. [9]

- A virus is when a computer or a system gets infected by an infected download. Sometimes a victim will click on a non- suspecting link or open an email from an unknown source. Once that happens, the "virus" is now inside your computer and can "infect" the system by either slowing down or shutting down the security features. Many times the person is unaware that the system has been affected. A virus can be introduced via what is known in the industry as a "Trojan Horse". Like the story of Troy, the virus hides behind something that looks legitimate to gain access and once inside can do damage or steal information. These viruses are sometimes called malware, short for malicious software. It is any software used to disrupt computer operations, gather sensitive information, gain access to private computer systems, or display unwanted advertising. Malware is defined by its malicious intent, acting against the requirements of the computer user, and does not include software that causes unintentional harm.

- Physical Theft accounts for about 20% of all large data breaches overall. Most occur within the healthcare system, accounting for over half of physical data theft. The largest to date physical data theft occurred when a laptop was stolen from a vehicle that belong to a Veterans' Administration Health System employee. Thousands of sensitive patient information was compromised through this theft.
- Skimming is a way of collecting credit card information. Criminals will put a card reading device over the original card reader of an ATM machine, a gas pump machine or any other self-service physical point of sale device. After a consumer uses the machine, the criminal then goes in after, removes the skimming device then downloads the financial information of the stolen cards. They either use these cards to make unauthorized purchases or sell the card information to a larger criminal operation.
- Phishing is a form of fraud in which the attacker tries to learn information such as login credentials or account information by masquerading as a reputable entity or person in email, IM or other communication channels. Often time masquerading as a bank, an email will be sent to a customer requesting to reset your account information, asking for pertinent information like social security numbers, PIN numbers and other Personally Identifiable Information.
- Social engineering is a type of psychological manipulation of people to divulge confidential information, gain system entry or initiate a cyber-attack. [6]

2.3 PERSONALLY IDENTIFIABLE INFORMATION (PII)

Personally identifiable information is a broad term used in the cyber industry and refers to any information that could be used to identifying a person. [5] This information could be a credit card or bank account numbers, which are referred to dynamic PII. Or the information is classified as fixed PII. This would include information such as social security number, date of birth or place of birth. Dynamic PII, once compromised can be changed. For example, if your bank card information has been breached, your bank will issue you a new bank card with a new account number. Although damage may or may not have been done due to this type of breach, the issuance of a new account number stops any further compromises to that account. On the other hand, Fixed PII is a person's permanent information and cannot be re-issued if breached or stolen. This type of information is critical to protect because there is no remedy once stolen.

2.4 RECENT SECURITY BREACHES [3]

- December 2013 – Target; Hackers stole credit and debit card information as well as email and mailing addresses of 70 million customers.
- July-August 2014 – JP Morgan Chase; Hackers gained access to JP Morgan Chase's database and stole customer information of some 83 million households and small businesses. They claim only home addresses and email addresses were stolen and no sensitive information was compromised.
- October 2014 – Staples; Hackers were able to get into the company's system and stole credit card information of 1.6 million consumers.
- November 2014 – Sony Picture; The salary lists, contracts, emails film budgets and Social Security numbers were stolen from Sony Pictures, leading to the cancellation of a big movie release. It was feared that North Korea was the culprit, though it was never proven as retaliation to the movie "*The Interview*" which was a parody comedy about a fictional assassination attempt on the North Korean leader Kim Jong-un.
- February 2015 – Anthem BCBS; The nation's largest health insurer claimed the records of as many as 80 million current and former customers as well as employees. Information that was stolen comprised of Social Security numbers, birthdays, addresses, income data and employment information.
- June 2015 – United States Government, Office of Personnel Management (OPM); Information on up to 18 million current, former and retired Government workers' and any person who may have dealt with a background check of employee's personal information was stolen by Chinese hackers. Social Security numbers, addresses, fingerprints and background checks were compromised.
- July 2015 – Ashley Madison: An online dating site that came to be known as the cheating site was hacked and the information of users was stolen and used to blackmail people. Some notorious people were outed as users of the site from politicians, pro athletes to movie stars.
- July 2015 – Army National Guard; Unrelated to the OPM breach, The Army National Guard's computer network was hacked and the sensitive information of all current and former National Guardsmen's wasompromised.

2.4. HOW TO PROTECT YOURSELF

Consumers have to be advocates for their own cyber safety, not just at home with personal computer use but with the amount of information is shared and with whom. Listed below are some ways individuals can protect themselves [6]

- Build a better password.
- Install virus protection software and update it as necessary.
- Never open email attachments from unknown sources, go directly to website by typing URL versus clicking on a link.

- Do not store payment information on retailer sites. It may take a few extra moments during checkout to re-input your credit card number but if their system is hacked, your credit card number is not stored. Opt for checkout as visitor.
- If transmitting sensitive information via email, choose to encrypt content. Send the recipient the pass code in a separate email, never in the same email.
- Be cognizant of the amount of personal information shared on social media. Criminals are constantly looking on social media for easy targets.
- Shred personal papers that contain PII.

2.5 ORGANIZATION RESPONSIBILITY

Organizations that hold consumer information have a huge responsibility to their customers. By recognizing that cyber security is a real threat, not just to the company but to their customers and suppliers and investors, an organization has taken the first step for taking responsibility. Prioritizing IT in the business model will ensure safety to the company's data safety and to the customers PII protection. Companies must establish a data loss protection plan and a protocol to follow in the event that a data breach occurs. [8]

The cost associated with cyber-attacks continue to grow. As technology continues to grow so will the need for more investment in improvements in security to thwart future data breaches. [2] Unfortunately, as more companies purchase cyber insurance, these newly incurred costs are trickled down through pricing and passed onto the consumer. [2] However, the value to the customer for building consumer trust with good security will more often than not take precedence over price increases. Organizations can leverage data privacy and security as a competitive advantage. [1]

2.6. Network Security Protection

2.6.1. Cloud-Based Storage and Usage

A company's choice to move their data to the cloud comes with an array of factors to consider; including but not limited to cost of the service, data security and accessibility of the data for employees. From a cost perspective, maintaining internal servers comes at the cost of space, hardware, and IT support. Many proponents of cloud-base business argue that it is a cheaper alternative, but "some industry analysts estimate the break-even point of leasing versus buying the software at about three years" [11].

From a data security perspective, the increased risk of confidential information being breached is one of the primary concerns. J. Carlton Collins, CPA and Technology Consultant, argues the opposite, however. "Cloud-based accounting systems don't actually store your data in a vapor mist in the sky; rather your accounting data are stored in world-class data centers with fortified concrete walls, steel doors, retina scans needed for entry, world-class firewalls, state-of-the-art anti-virus technology, continuous backups, and often a mirrored backup of the entire data center" [12].

Assuming Collins' argument holds true, companies are actually benefitting from the security cloud-based services can provide. It should go without saying, however, that the level of security will differ from the various services. In the aftermath of the Target data breach, executives eventually disclosed that "security software detected potentially malicious activity, but its staff decided not to take immediate action [16]." Hindsight is always 20/20, but perhaps Target would have benefitted from having a third-party security company monitoring their networks.

2.6.2. Establishing a Virtual Private Network Connection

A good balance of data accessibility and data security comes in the form of a virtual private network (VPN) connection. "Using VPN software to encrypt information while it is in transit over the Internet in effect creates private communication channels, which are accessible only to those parties possessing the appropriate encryption and decryption keys" [10]. Using this alternative, data that lives on secure servers within the company's infrastructure could still be accessed directly by employees on the go. To establish the VPN connection, the employee would be required to authenticate their credentials before gaining access to the network.

With confidentiality being paramount in when client credit card information is involved, a two-factor authentication would be recommended. For example, an employee attempting to access the network remotely would first be prompted for their username and password. Once provided, a randomized and expiring pass code would be sent to them via text or email. Once entered, a VPN connection would be established and the employee could gain remote access to their typical network drives and programs.

In Target's data breach, the security credentials for the HVAC company may not have been enough to access the network had there been a two-factor authentication process in place. According to one source, "Only the vendors in the highest security group — those required to directly access confidential information — would be given a token and instructions on how to access that portion of the network. Target would have paid very little attention to vendors like Fazio (the HVAC company), and I would be surprised if there was ever even a basic security assessment done of those types of vendors by Target [17]."

2.6.3 Network Segmentation

If Target's payment systems had been properly isolated from other systems – a process called network segmentation – the data breach never would have happened [15]. Through network segmentation, systems containing credit card information would have been isolated from non-payment systems. When Target was hacked, the initial access point was through the HVAC system, but because the network was not segmented, the hackers were able to work through the network until they were eventually able to gain access to the payment systems.

One way of breaking a larger network into smaller sections is by implementing virtual local area networks (VLANs) [18]. Each VLAN can act independently while also remaining connected to the overarching network of the company. This process does come with its own set of risks, however. According to security experts, if a single port on a network is not configured correctly, intruders can break through from one virtual network to another [15]. As the network becomes more and more complex, the margin for error grows proportionally along with the potential for security gaps.

II. Privacy Data Security Protections in the U.S. HealthCare Industry

In the last five years, there have been numerous security breaches in the cyber world. From financial breaches of a retailer's credit card databases to sensitive medical information of patient of a healthcare network to the personal information. New technology continuously improves the ease with which the world communicates with and connects with each other, and with this ease and convenience comes potential dangers that we as consumers must be aware of.

3.1. U.S. Healthcare Information Technology Legislation

We live in a world of ever-changing technology, which has its advantages and disadvantages as well as challenges and issues that must be addressed. When it comes to the healthcare industry, organizations must consider a patient's privacy and security concerns. By changing from paper to electronic health records patient's information is vulnerable to security breaches. It is important to have confidentiality, integrity, and available of all electronic health records. Creating a comprehensive security system is the key to avoiding data breaches and gaining a patient's trust in your security system. To make adequate changes, the country as a whole must ban together and passes legislation that creates standards for all healthcare organizations to follow.

3.1.1. American Recovery & Reinvestment Act

On February 17, 2009, President Barack Obama signed the American Recovery and Reinvestment Act. He wanted the American people to understand that this was only the beginning by stating, "The road to recovery will not be straight. We will make progress and there may be some slippage along the way. It will demand courage and discipline. It will demand a new sense of responsibility that's been missing." [25]

The American Recovery and Reinvestment Act, also known as the recovery act, addressed numerous different areas of concern including the economy, education, renewable energy, and governmental programs that provide assistance to many Americans. The act also addressed healthcare. The goal was to find a way to provide affordable healthcare to all citizens and to use today's technology as a tool to provide doctor's with accurate and up-to-date information regarding their patients. In order to do this, organizations were required to increase access to informational technology with better methods of storing, analyzing, and sharing any and all health information.

3.1.2. Health Information Technology for Economic & Clinical Health Act

In an effort to promote health information technology, the Recovery Act included the Health Information Technology for Economic and Clinical Health Act, or HITECH. The ultimate goal was to create an infrastructure that allowed health care workers including hospitals, physicians, and other treatment centers, the ability to share information quickly and accurately. In order to ensure that healthcare organizations followed all laws, standards, and other mandates, the Recovery Act also formally established the Office of the National Coordinator, or the ONC, to oversee health information technology. In conjunction with the ONC, the Health Care Authority monitors HITECH grant programs to ensure that all standards are being met on a state level as well. [22]

3.1.3. Health Insurance Portability Act

Another legislative act passed that coincided with the American Recovery and Reinvestment Act is the Health Insurance Portability and Accountability Act. The Portability and Accountability Act requires all healthcare organizations to protect the interest of their patients. The act was first passed in 1996 by President Bill Clinton but was later readdressed in an effort to maximize today's technology. It was back in 1996 that healthcare organizations were required to meet certain national standards when they were transmitting health data electronically.

As you can see many initiatives have been created in the health information technology field to ensure patient privacy and security when healthcare organizations collect and store patient information electronically. These acts are just the tip of the iceberg when it comes to the number of laws created in this field, but there is still more work that needs to be done and, in turn, more legislation that will need to continue to expand as technology reaches new heights.

3.2. Paper Records vs. Electronic Health Records

For many years, physicians and other members of the healthcare family kept all medical records on paper. This meant that every time a patient came to the office someone would have to find that file and provide it to the physician. Overtime, as the number of patients, files, and file sizes grew so didn't the required storage space and personnel needed to maintain all of them. With this system if a patient called in and had a question about their medical history it could take a long time for the staff to locate the file and sort through all the paperwork to locate the correct information. This was not only costing an employee's time, but also financial costing more for the physician or healthcare organization.

Thirty years ago, this was the norm and people didn't think twice about it, but now we have access to quickly growing technologies that we can utilize to make the healthcare profession more efficient and, in turn, provide better service to their patients.

In 2001, we began to see healthcare practices utilizing information technology by creating electron health records or EHRs. Organizations saw the benefits of streamlining their records into one system that made file cabinets full of files obsolete. Electronic Health Records allowed physicians to quickly access a patient's medical record and provided the most up-to-date information on their medical history at their fingertips. Doctors therefore, could see more patients as they were not trying to sort through a potentially large file with their entire medical history. An electronic record allowed a doctor to locate specific information quickly and avoid irrelevant data.

3.3. Security Components for Electronic Health Records

Multiple components are necessary to have adequate security of all electronic health records. Without each component, an organization is leaving itself wide open for numerous different securities breaches. Like an intricate clock, all components are required for a system to function properly.

These items include hardware, software, updated procedures, and properly trained personnel.

Hardware has the capabilities to provide an organization with three things that a human cannot: speed, accuracy, and storage capabilities. Their speed allows them to complete requested tasks quicker. Using a computer increases accuracy when compared to humans. Creating safety measures that help reduce the probability that users enter incorrect data not only increases accuracy but provides an additional safe guard for patient records. Finally, a computer's hardware provides storage capabilities that allow users to save large quantities of data while still being able to retrieve data almost instantly.

A single computer can store data equivalent to a large storage warehouse filled with filing cabinets of patient records. To some people a computer's hardware can seem simplistic when it comes to maintaining electronic health records but many components are so common that people may forget they exist. A computer's hardware is more complicated than connecting a tower to a monitor, inside that tower is many parts that power that computer and the structure once you plug it into a power outlet. For example, inside each tower is a hard disk drive which handles all the storage needs necessary for that device. One hard drive may be divided into different sections called partitions. Regardless of how a hard drive is physically constructed it still controls a computer's software, which is another component in creating an adequate security system on a computer. [21]

Without software to utilize a computer's hardware, the hardware is essentially useless. A computer's software is all the programs that run in the background and provide a system with such tasks as deleting unnecessary data and maintaining stored files. Healthcare organizations utilize application software which performs specifically designed tasks to meet their needs. The problem arises with the lack of standards and policies in the construction of records management software, but last October a step was made in the right direction.

In October 2015, twelve of the leaders in electronic health records developers agreed to "a set of objective measures of interoperability and ongoing reporting" [24]. The reporting will help track differences between vendors and how that affects patients Information gathered will also be used to send general reports to governmental agencies to demonstrate changes in the market. The push for standards comes after many developers faced criticism over the months prior to the meeting in regards to the lack of interoperability of medical records after the government invested $31.5 billion federal dollars. [24]

Lastly, a security system must have updated procedures to ensure that access is only granted to certain users and that data is remaining confidential. One procedure that is common before someone is granted access is running a background check on the individual. This can help filter out individuals that may create a security risk for an organization. Furthermore, creating a policy that requires a user to sign in and out of a workstation if they leave their workstation for even a minute is another policy that should be enacted. This warrants against any unauthorized users from obtaining confidential information. In order to make sure that they are followed, an organization's administration must select adequate personnel that will value a patient's privacy and the value of the information located on their computer systems.

3.4. Confidentiality, Integrity, and Availability

Three of the most important aspects of network and computer security are confidentiality, integrity, and availability, also known as the CIA triangle. To meet confidentiality measures the rule is straightforward; a system must not allow any information to be disclosed. In the healthcare industry most if not all of the information collected from patients is considered confidential. The integrity portion of the CIA triangle states that accurate data must be used within the system. This includes making sure that authorized or unauthorized users are not making inaccurate changes to any files. Lastly, available means information can be easily accessed in a system and that there are enough workstations so that any authorized user can access the system without having to wait for someone else to finish. Availability also means that a system can quickly be recovered if there is a system failure. [20] All three components are essential in creating a top notch system to store electronic health records.

3.5. Data Encryption

Data encryption occurs when data is encoded in a way that is unable to be deciphered by unauthorized users. However, interception is not prevented with data encryption; it just means the receiver of the data will be unable to read the contents. Even with the legislation that has been passed over the last fifteen years, those collecting and storing sensitive health information are not required to encrypt their data. The Health Insurance Portability and Accountability Act only encourages the use of encryption.

One well-known example occurred just last year with the second largest health insurer in the United States, Anthem. Anthem's security breach allowed hackers to gain access to over 80 million Americans information that included some former members as well as nonmembers, as Anthem managed paperwork for small independent insurance companies. The problem with Anthem's securities system is that the failed to encrypt a large amount of personal data they stored, that most victims were unaware they kept that information on files. When investigated, it was believed that the hackers collected credentials to at least five employees that had high-level IT clearance through phishing.

The major problem is the hacker was able to phish multiple high-level IT employees without being detected by their security software or by other employees. Due to the lack of security in guarding confidential information it meant that in this instance an employee who was the one to eventually detect the breach. Anthem claims that they believed the breach went on for weeks, which could of potentially have been prevented if a comprehensive security system was in place, which included encrypted data. [26]

Even after the security breach at Anthem occurred, there still has not been legislation passed that requires all electronic health records be encrypted. Just this month the Federal Trade Commission sued Henry Schein Practice Solutions who sells software for dental practice management for "allegedly mispresenting its level of encryption for patient data". [20] However, the Federal Trade Commission was not suing because of a data breach, but rather because the software was misrepresented.

The company's Dentrix G5 software claimed that it utilized industry-standards encryption when it actually used an inferior method. This was determined by the Advanced Encryption Standards, which are recommended by the National Institute of Standards and Technology. [20] This move by the Federal Trade Commission is a move in the right direction but, more needs to be done to regulate data encryption in healthcare.

3.6. Patient's Control over Electronic Data

In order to operate a success healthcare organization, that organization must gain and maintain a patient's trust. Studies have shown that due to the advances being made in technology that some patients have failed to seek treatment or they do not disclose all necessary information required to adequate treat them. One reason this occurs is because patients have a lack of trust in the way their confidential information is collected and stored. Many patients are seeking to have greater control over their personal information.

We are starting to see a shift towards patients having control over their medical records through online websites associated with healthcare organizations. Patients use their username and password to log into the website and can access their personal information, send a message to their physician, request medication refills, and set up appointments. [23]. However, these types of websites are new to the medical field and, therefore, are structured differently since there are currently no standards to monitor them. These types of systems can be found in larger organizations, but we have a long way till we see them in all organizations as they systems are costly to create and maintain.

III. Conclusion

As technology continues to evolve, so does the threat. As a society, we cannot afford to become complacent and lazy. We cannot rely on the technology itself to protect us. It is our responsibility as individuals and organizations to be vigilant and ever evolving with the changing times. The connectivity of the World Wide Web is an amazing function, but it opens up a world of vulnerability. It is possible to enjoy the fruits of innovation as long as we stay informed, educated and aware. Take the IT discussion seriously, view the training offered by employers as an opportunity to increase your cyber competency. With safety as a forefront, consumers and business alike can expect to experience a rewarding existence in the cyber world.

As anticipated, steps have been made to improve the way we use technology in healthcare, but were still years away from creating a more secure and interoperability system. The problem lays in the lack of standards and legislation behind electronic health records and the corresponding software. Also, more needs to be done to ensure the security of confidential information so that customers/patients feel comfortable sharing information with business/medical workers.

In more details of medical industry, creating a cohesive system to store medical records that patients can trust will hopefully one day mean that patients will be willing to be involved in different research in order to cure and possibly prevent certain diseases and conditions. Ultimately, the software behind electronic medical records needs to place patients first and foremost.

Even with all the security out there, the sad reality is that network protection is usually a step behind the hackers. If a hacker group wants data bad enough they will most likely be able to find a way to crack the system assuming they have enough knowledge to do so. Nonetheless, security companies continue to adapt and build security systems that help to ward off hackers and protect the data of their clients.

In the case of the Target data breach, one could argue it was the company's own hubris and/or stupidity that eventually resulted in the breach. The system in place was properly alerting their security team of malicious behavior but those involved chose to ignore it. The result is millions of dollars in fines and damages that the company must now pay.

Coincidently, many hackers groups are not driven by the monetary aspect but rather, the ability to impose change within big businesses. A hacker group may acquire confidential data from a company and make demands while threatening to expose the data to the public. This holds true with the data breach of the online dating service, Ashley Madison. The group has claimed two motivations: First, they've criticized Ashley Madison's core mission of arranging affairs between married individuals. Second, they've attacked Ashley Madison's business practices, in particular its requirement that users pay $19 for the privilege of deleting all their data from the site (but, as it turns out, not all data was scrubbed) (Hackett, 2015).

In closing, the internet is not showing signs of going away anytime soon. It is a gift and a curse that the internet allows us to stay connected. On one hand the internet allows us to communicate with family members across the globe, or access the world's knowledge with one click. On the other hand, a hacker could have remotely accessed my desktop and is watching me type each and every word of this paper without my knowing. For better or worse, we just try to tell our self that our life is boring enough that a hacker wouldn't want anything to do with us anyways, so we just try and go about my life as if we are immune to it all. As they say, ignorance is bliss.

References

[1] Conroy, P., Milano, F., Narula, A., and Singhal., R. (2016). Building Consumer Trust: Protecting Personal Data in the Consumer Product Industry. Deloitte University Press. N.p., 13 November, 1-28.

[2] Ford, T. (2014). Cyber Attacks and Their Impact on Business. GlobalEDGE Blog: GlobalEDGE: Your Source for Global Business Knowledge. N.p., 11 June 2014. Web. 11 Feb. 2016.

[3] Granville, K. (2015). 9 Recent Cyberattacks Against Big Businesses. The New York Times. The New York Times, 04 Feb. 2015.

[4] Simberkoff, D. (2014). Cyber Security Is a Shared Responsibility - AvePoint Community. AvePoint Community. AvePoint, 07 Oct. 2014. Web. 11 Feb. 2016.

[5] Weiss, A. (2014). How to Protect PII. - ESecurity Planet. ESucurity Planet, 15 May 2014. Web. 11 Feb. 2016.

[6] Zaharia, A. (2015). 10 Surprising Cyber Security Facts That May Affect Your Online Safety - Heimdal Security Blog. Heimdal Security Blog. N.p., 25 Mar. 2015. Web. 11 Feb. 2016.

[7] Cyber Security Primer. (2016). What Is Cyber Security? Department of Homeland Security, n.d. Web. 11 Feb. 2016.

[8] Data Breach Prevention Tips. (2016). Data Security Best Practices. N.p., n.d. Web. 11 Feb. 2016.

[9] The 3 Most Common Types of Data Breaches - And How to Prevent Them - 20s Money. (2015). 20s Money. N.p., 30 Jan. 2015. Web. 11 Feb. 2016

[10] Romney, M.B., Steinbart, P.J. (2015). Accounting Information Systems. Harlow, England: Pearson Education Limited.

[11] Defelice, Alexandra. (2010). Cloud Computing: What Accountants Need to Know. Journal Of Accountancy. 10 Oct. 2010. Business Source Premier. Web. 10 Jan. 2016.

[12] Collins, J. Carlton. (2015). Online accounting systems: Accounting for cloud security. Journal Of Accountancy. 1 Sep. 2015. Business Source Premier. Web. 10 Jan. 2016.

[13] Robin Sidel. (2015). Target to Settle Claims Over Data Breach. Wall Street Journal. 18 Aug. 2015. Web. 10 Jan. 2016.

[14] Jeffrey Jones. (2015). In U.S., Telecommuting for Work Climbs to 37%." GALLUP. 19 Aug. 2015. Web. 10 Jan. 2016.

[15] Rachael King. (2014). Isolating Cardholder Data May Have Prevented Target Breach. Wall Street Journal. 10 Feb. 2014.

[16] Jim Finkle & Susan Heavey. (2014). Target says it declined to act on early alert of cyber breach. Reuters. 13 Mar. 2014. Web. 10 Jan. 2016.

[17] Email Attack on Vendor Set Up Breach at Target. KrebsonSecurity. 12 Feb. 2014. Web. 10 Jan. 2016.

[18] Cisco Networking Academy's Introduction to VLANs. (2016). Cisco Networking Academy. 7 Apr. 2014. Web. 10 Jan. 2016.

[19] Robert Hackett. (2015). What to know about the Ashley Madison hack. FORTUNE. 26 Aug., 2015.

[20] Bidgoli, Hossein.(2013). MIS3. Boston, Etats-Unis: Course Technology, Cengage Learning, 2013. Print. Caspi, Heather. FTC Takes On Watchdog Role, Settles Data Encryption Case For $250K. Healthcare Dive.

[21] Fisher, Tim. (2016). What Is A Hard Drive? About.com Tech. N.p., 2016. Web. 30 Jan. 2016.

[22] Hca.wa.gov, (2016). Health Information Technology Overview. N.p., 2016. Web. 28 Jan. 2016.

[23] Medical Economics. (2016). First Take: Medical Records Belong To Patients. Period. N.p., 2016. Web. 31 Jan. 2016.

[24] Modern Healthcare, (2016). Vendors Agree On Interoperability. N.p., 2016. Web. 1 Feb. 2016.

[25] The White House. (2016). About The Recovery Act. N.p., 2016. Web. 28 Jan. 2016.

[26] Times, Los. (2015). Anthem Is Warning Consumers About Its Huge Data Breach. Here's A Translation, latimes.com. N.p., 2015. Web. 31 Jan. 2016.

AUTHORS

First Author – Kay K. Kim, Fitchburg State University, Fitchburg MA 01420 USA, kkim@fitchburgstate.edu