IOSR Journal of Economics and Finance (IOSR-JEF)
e-ISSN: 2321-5933, p-ISSN: 2321-5925.Volume 5, Issue 6. Ver. III (Nov.-Dec. 2014), PP 36-45
www.iosrjournals.org

Data Breaches and Identity Theft: Costs and Responses

Rita O. Koyame-Marsh and John L. Marsh

I. Introduction

Today's online world brings new challenges to organizations such as protecting people's information as transactions of various kinds with a variety of private vendors, government agencies, and even with one another are stored electronically in databases or on personal electronic devices. These databases and electronic devices are vulnerable to attacks by hackers who could gain access to millions of people's personal information and sell them to the highest bidder. In addition to hackers, personal information can be stolen by those with legitimate access to databases for work purposes. Medical network systems are among the top places where people's most intimate information can be found and stolen. People's personal information is usually stolen for identity theft goals where information required for identifying an individual such as name, birthdate, address, and Social Security Number(SSN) can be used fraudulently.

Datasecurity breaches that could lead to identity theft are just a click away as computer networksystemsbecome more and more vulnerable fromattacksby hackers and viruses. Databases are also accessed daily by workers who have the potential of misusing people's private information for financial gains.Discoveringprivate information about someone is even easier today andcan occur anywhere access to medical or personal information exists. Unlike the days before laptops and personal data storages devices, current technology makes it possible to download thousands of records into a single handheld device or take pictures of information appearing on computer screens or paper forms in a few seconds.

Complaints about identity theft have been on the rise since 1997 when the Federal Trade Commission (FTC) startedto keepcount. The Consumer Sentinel Network (CSN) of the FTC reported that, between January and December 2013, they received more than2 million consumer complaints of which 14% (about 290,056 complaints); the highest number of complaints,was from the identity theft category (CSN, 2014)[1]. Identity theft is also becoming increasingly costly to American people.It was estimated, on the basis of a 2006FTC's Identity Theft Survey, that the total amount stolen in 2005 by identity thieves from victims was about $15.6 billion with 8.3 million of U.S. adults becoming victims of some types of identity theftthe same year (Synovate, 2007). The amount stolen rose to about $18 billionin 2013 with13.1 million of U.S. adult becomingvictims of identity fraud in that same year(Javelin, 2014).

The dollar estimates of the cost of identity theft do not by themselves indicate how muchidentity fraud is occurring. However, press accounts of data breaches suggest that personalidentifying data (PID) are being stolen very frequently, and that the data thefts are undulyfacilitating various kinds of identity theft (See Acohido, 2013; Cardenas, 2013).There is also a general sense that "too much" PID is beingcollected, though some suggested policy fixes imply that more, not less, PID should be collectedas a deterrent against its potential misuse. Identity theft is big news and a big business today. It requires just a few pieces of information about someone to open accounts, file taxes or invoice false medical claims. Information theft is also in the news as public figure's phones or social web sites are hacked and their text messages and other information are released to the public. The mother-load of personal information is contained in one's medical records where unfortunately SSNhas been used as a convenient unique identifier because it is unique and patients have it memorized. Medical records contain address, age, SSN, and government IDs such as Medicare Number as well as the medical history itself. The latter might not seem as important, but consider the value of such information for a famous celebrity. There is a street value for all of these pieces of information. For example, to those involved in tax fraud, SSNs for the very young and very old are most valuable because those individuals aren't likely to file tax returns of their own which would raise an immediate investigation. SSNs of people not filing their own returns can be used fraudulently unnoticed for several years.

Moreover, the fall in the cost of information technology is causing more and more personal data to be collected and stored. While collecting and storing such data undoubtedly provides economic benefits, it has proven impossible to keep data completely secure against criminal misuse. Our personal information must necessarily be guarded from tampering because they are used to assess our credibility, who we are, and what we have done in society. Any inaccurate information about a person as a result of identity theft can be costly because one can be denied a loan, a job, or even a place to rent among other things.

[1] CNS is a secure online database of millions of unverified consumer complaints received by the FTC and some state law enforcement organizations.

Several laws had been enacted by the U.S. federal and state governmentsin response to the concern of identity theft and information abuses. For instance,the 1996Health Insurance Portability and Accountability Act (HIPPA) and the 2009 Health Information Technology for Economic and Clinical Health Act (HITECH),were enacted to govern the use and exchange of health information as well as notification responsibilities when privacy breaches occur (DHHS, 2013).The 1998 Federal Identity Theft Assumption and Deterrence Act (ITAD) which, among other things, mandatesthe FTC to create a central depository for complaints of identity theft and offer assistance to victims. Additional laws and regulations regarding identity theft will continue to be enacted through the years as identity theft becomes more and more prevalent and identity thieves become more sophisticated in their criminal activities. S.149: Stop Identity Theft Act of 2013 is the latest example of new laws and regulations being enacted by the U.S. federal government.

Private companiesare also doing their part in addressing the problems of data security breaches and identity theft by, for instance, educating their employee about data breaches and establishing anti-theft monitoring services. One of the authorsof this study has recently done consulting work for a very large healthcare system of hospitals and physician network in the United States. The latter wanted to respond to the threat of information theft from an information technology perspective. This healthcare organization had at that time about 20,000 identified users in their system thathad access to varying amounts of patient information. There were also other users in offices of affiliated businesses accessing patient information using an access login that is shared among several people that werenot specifically identified. Access to patient information was not limited to hospital employees or other employees of the organization, but, was also available to outside physician offices, ambulance companies, medical billing companies, and so on. Each company has legitimate reasons to access patient’s personal information, and is a potential point of extraction for an individual’s most intimate information as well as key identifying information such as SSN or Medicare Number.

This paper examines the technological response to data breach and information theft by a healthcare system. It also discusses the potential economic costs of data breach and identity thefts to U.S. individuals, businesses, and governments. The paper is organized as follows: section 2 reviews the literature while section 3 gives an overview of data breaches and identity theft. Section 4 discusses the economic costs of identity theft and data breaches. Section 5 presents the different types of data breaches faced by a medical organization and discusses the latter’s response to the threat of data security breaches and information theft. The paper ends with a conclusion in section 6.

II. Literature Review

Theliterature on data breaches and identity theft is not as broad due to the novelty of these topics. The following are some of the latest studies on data breaches and identity theft: Lai et al. (2012), Robert and Schreft (2009), Anderson et al. (2008), Solove (2008),Schreft (2007), Anderson (2006), Kahn and Roberds (2005), and Cheney (2005).Lai et al. (2012) used coping behavior theories to empirically examine the role of both the conventional coping and the technological coping behaviors in combatting identity theft. They use the structural modeling approach and test the model using data collected from a survey of 117 respondents. They found that both types of coping behaviors effectively help fight identity theft.

Roberds and Schreft (2009) studied the implications of networks’ collection of personal information data, data security, and costs of identity theft using a monetary-theoretic model. They found that too much data collection and too little security arise in equilibrium with non-cooperative networks compared with the efficient allocation. They also analyze a number of potential remedies to the problems, remedies such as mandated security levels and data-breach costs reallocation. Anderson et al. (2008) discussed the prevalence and cost of identity theft using surveys conducted by the FTC in 2003 and 2006. They also explained the institutional framework in which identity theft occurs and discussed some policy issues.

Solove (2008) arguedthat the lack of regulations in the management of personal information by companies is the cause of abuses of personal information. He claimed that, even though companies take intricate technological measures to protect their data systems, theystand ready to distribute personal informationcollected to other entities and occasionally to anyone for a fee. To effectively curtail personal information abuses, the law should address information leaks and insecurity which are the main causes of information abuses.

Schreft (2007) examined the nature of identity theft and looked at the factors that led to its growth. The paper also examined whether or not the markets for goods and services could limit the risk that identity theft poses to the payment system and found that the markets fail to curtail this risk due to existing market imperfections. Government regulations are needed to protect the integrity and efficiency of the payment system in order to overcome market failures. Anderson (2006) used the FTC's 2003 identity theft survey data to examine the likelihood that a person might experience identity theft based on their demographic characteristics. It was determined that there is a higher risk of identity theft for women, younger consumers, and people with higher incomes. In addition, the number of noncash accounts the consumer has and the intensity of their use may increase a person’s risk of becoming a victim of identity theft.

Cheney (2005) discussed the differences among financial frauds associated with identity theft which he believed necessitate additional distinction and treatment by consumers, lenders, financial institutions, and law enforcement agencies in order to better understand these kinds of criminal behavior. Cheney distinguished four types of financial fraud that all fall under the legal term identity theft: fictitious identity fraud, payment card fraud, account takeover fraud, and true name fraud. The author believes that further definitional descriptions of identity theft would be beneficial indeveloping effective solutions to the problem.

Kahn and Roberds (2005)studied identity and its use in credit transactions to find the equilibrium incidence of identity theft. The latter represents a tradeoff between, on one hand, the necessity to control transaction fraud and on the other hand thewish to avoid costly or intrusive monitoring of individuals. The results of this study indicate that advances in technology will not curtail this tradeoff and that several types of identity theft such as friendly fraud,existing account fraud, and new account fraud happen in equilibrium.

This study differs from previous ones because it presents a specific case study of a healthcare organization as it responds tothe threat of medical information theft. In addition, it discusses the economic costs of data breaches and identity theft using the latest data available.The case study presented here is based on consulting work done by one of the authors of this study, while the discussion about the economic costs of data breaches and identity theftis based on data provided by the 2006 FTC’s Identity Theft Survey Report (Synovate, 2007) and the 2014 Javelin Strategy & Research Study (Javelin, 2014). The 2006 FTC’s Identity Theft Survey Report was based on a total of 4,917 telephone interviews of U.S. adults age 18 and older conducted by the FTC between March 27 and June 11, 2006 using a Random-Digit-Dialing (RDD) sampling methodology.Javelin Strategy & Research 2014 study conducted an address-based survey of 5,634 U.S. consumers in 2013 to determine the impact of identity fraud.

III. Data Breach and Identity Theft: An Overview

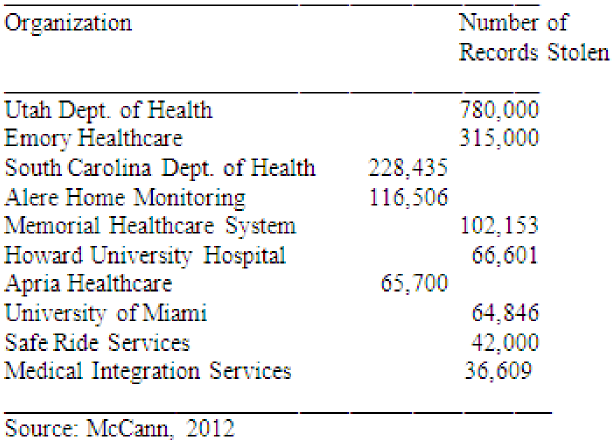
Identity theft can take many forms inpractice and need not involve data breaches. Identity theft is defined both by statute: ID Theft Act, 18 U.S.C. § 1028(a) (7) and § 1029(e) (FTC, 1998) and by FTC rules: 16 C.F.R. § 603.2 (FTC, 2007). It includes the misuse or attempted misuse of any identifying information – such as the SSN, biometric data, or an existing credit card account number to commit fraud. The 2006 FTC’s Identity Theft Survey Report dividesidentity theft into three broad categories: Existing Credit Card Only, Existing Non-Credit Card Account, and New Accounts & Other Frauds. “Existing Credit Card Only” fraud occurs when a thief steals a credit card number and uses it to purchase goods and services. “ExistingNon-Credit Card Account” fraud occurs when a thief steals existing payment account information(e.g., a checking account number) and uses it to purchase goods and services. “New Accounts & Other frauds” occur when a thief uses someone else’s PID to open a new account.

Identity theft is an evolving crime.Anincreasingly prevalent type of “New Accounts & Other Frauds”is a fictitious or synthetic identity fraud, in which athief combines information taken from a variety of sources with invented information to create anew fictitious identity that he or she uses to open a new account.In addition, identity fraudsters are now more than three times as likely to use the money stolen to buy prepaid or gift cards to make fraudulent purchases.Moreover, account takeover reached a new record for the second year in a row, accounting for 28 percent of identity fraud losses in 2013. Among account takeover frauds, those for utilities and mobile phone almost tripled, as criminals add new properties to victims’ utility accounts and run up unauthorized phone charges. Non-card frauds,which include compromised lines of credit, Internet accounts (e.g., eBay, Amazon) and email payment accounts such as PayPal, also saw a rapid rise in 2013. Non-card fraudsaccounted for about $5 billion in fraud in 2013 and it affected triple the number of consumers when compared to 2012 (Javelin, 2014).

A data breach is neither a necessary nor a sufficient condition for identity theft, but it can facilitate either existingaccount fraud or newaccount fraud.There is no definitiveestimate of how many cases of identity theft have resulted from data breaches. It is,nevertheless, plausible to expect a higher number of identity frauds as data security breach occurrences increase. According to theinformationsecurity website Attrition.org, there were 326 worldwide incidents of data breachin 2007 which resulted in 162 million personal data records compromised compared with only 11 reportedincidents in 2003 with 6 million compromised records (Jewell, 2008). These figures are likely to be underestimated asmany breaches are not reported.

Javelin (2014)stipulated that data breaches currently represent the greatest risk factor for identity fraud.One in three consumers who received notification of a data breach in 2013 became a victim of fraud compared to one in four in 2012. In addition, 46 percent of consumers who had breached debit cards in 2013 became fraud victims in the same year while only 16 percent of consumers with a breached SSN became victims of fraud in 2012. An increasingly higher number of data breaches have also been occurring in the healthcare industry. Table 1 shows the top 10 medical information breaches of 2012.

Table 1: Top10 Healthcare Information Breaches of 2012



Organization	Number of Records Stolen
Utah Dept. of Health	780,000
Emory Healthcare	315,000
South Carolina Dept. of Health	228,435
Alere Home Monitoring	116,506
Memorial Healthcare System	102,153
Howard University Hospital	66,601
Apria Healthcare	65,700
University of Miami	64,846
Safe Ride Services	42,000
Medical Integration Services	36,609

Source: McCann, 2012

IV. Economic Costs of Identity Theft and Data Breaches

Identity theft imposes economic costs not only to individuals but also to businesses and thegovernment. Identity theft is even more costly to individuals when we addindirect costs such as the opportunity cost of time spent resolving problems caused by identity fraud and out-of-pocket costs incurred by victims to resolve thecrime which may include legal fees,lost wages, payments of any fraudulent debts, and other expenses such as postage and notarization fees.

Asidentity thefts become more prevalent and identity thieves more sophisticated in their crime, one should expect the costs of identity theft to rise overtime unless measures taken toprevent and combat such crime also evolve overtime.According to Javelin (2014),the dollar amount stolen from identity fraud decreased from $21 billion in 2012 to $18 billion in 2013indicatingperhaps more aggressive actions from financial institutions, consumers, and identity theft protection providers.

Fraud Victims and Out of pocket costs

As previously mentioned, the total amount stolen by identity thieves from victims in the U.S. wasabout $18 billion in 2013. In addition, more and more people are becoming victims of identity fraud as transactions are increasingly being conducted using electronic devices and more and more PID are stored in these devices. For instance, the number of identity fraud victims increased by 500,000 between 2012 and 2013 to 13.1 million people (Javelin, 2014).

Fortunately, victims of identity theft are not, in most cases, legally responsible for the cost of fraudulent transaction by thieves that misuse their personal information. A variety of laws limit consumers' liability in these situations. The FTC's 2006 survey reported that 59% of victims of identity theft incurred no out-of-pocket expenses in 2005. While some victims did incur substantial out-of-pocket expenses, the median value of out-of-pocket expenses was about $40in the New Accounts & Other Frauds category. The top10 percent of all identity theft victimsreported out-of-pocket expenses of $1,200 or more. For the New Accounts & Other Frauds category, the top 10 percent of the victims incurred expenses of at least $3,000, and the top 5 percent incurred expenses of at least $5,000. One-quarter of victims in the New Accounts &Other Frauds category reported at least $1,000 in out-of-pocket expenses (Synovate, 2007).

Indirect Costs to Consumers

While most identity theft victims don't incur any out of pocket expense, the indirect costs associated with identity theft can be substantial. For instance, if the credit score of a victim is negatively affected as a result of identity theft, he or she will incur additional economic costs that may come in the form of a denied loan and/ora denied job due to bad credit. In cases where a loan is procured, a victim of identity theft might still be charged higher interest rate due to a lower credit score. The 2006 FTC survey reported the following (Synovate, 2007, P. 7):

"Thirty-Seven percent of ID theft victims reported experiencing problems other than out-of-pocket expenses or the expenditure of time in resolving issues as a result of having their personal information misused. The problems victims reported include, among other things, being harassed by collections agents, being denied new credit, being unable to use existing credit cards, being unable to obtain loans, having their utilities cut off, being subject to a criminal investigation or civil suit, being arrested, and having difficulties obtaining or accessing bank."

The opportunity costsof time spent repairing one's credit can't be overlooked either. Indeed, victims of all types of identity theft spent countless hours resolving the various problems as a result of identity theft. The median value for the number of hours spent resolving problems by all victims of identity theft in 2005 was 4. However, the top 10 percent of all victims spent at least 55 hours resolving their problems while the top 5 percent spent at least 130 hours. Victims in the New Accounts & Other Frauds category spent the greatest amount of timeresolving problems, 100 hours or more for the top 10 percent of victims in this category and at least 1,200 hours for the top 5 percent of victims (Synovate, 2007).

To try to limit the adverse impact of identity theft on a victim's credit score, the Fair Credit Reporting Act (Fair Credit Reporting Act § 605A(b), 15 U.S.C. § 1681c-1(b)) has, as of December 2004, allowed consumers who have a good faith suspicion that they have been or might become victims of Identity theft to place an initial "fraud alert" on their credit file(FTC, 2012). The fraud alert will appear on credit reports issued to potential users of the report notifying them that the consumer may be a victim of identity theft. The latter stays in place for a period of 90 days. A potential creditor is compelled to take reasonable steps to verify the identity of the person applying for credit when they receive a credit report containing a fraud alert.When a consumer becomes a victim of identitytheft, the Fair Credit Reporting Act allows him or her to place an extended, seven-year fraud alert on his or her credit file. The extended alert appears on all credit reports about the victim, notifying any potential user that the consumer has been a victim of identity theft. The extended alert also contains a telephone number at which the consumer may be reached. Any potential creditor must contact the consumer either at the provided telephone number or in person before extending any additional credit in the consumer's name. Some states have allowed victims of identity theft to request a "credit freeze," which prevents their credit reports from being accessed without their consent.

Costs to Companies

Data breaches and identity theft not only cost money and time to individuals but also to companies in lost goods and services, lost business, prevention of data breaches, and response to data breaches. Since most of the customers who becomevictims of fraud are not required by laws to pay for what the identity thieves have stolen, businesses absorb these losses. In addition, companies are spending more time and money to prevent information breaches from their database as hackers become more and more sophisticated in their operations and information breaches become more and more frequent (e.g. Cases of Target, eBay, TJ Maxx, and others). In fact, businesses not only need to make their database more secure butalso have to constantly improve their security system to be a step ahead of hackers.

According to Ponemon Institute's 2014 study on Global Cost of Data Breach, the primary root cause of the data breach in most countries and the most costlyis a malicious insider or criminal attack (Ponemon Institute, 2014)[2]. Currently, small companies have been averaging about 50 malware alerts per week, while a large globally dispersed company can have on average about 97 activeinfected assets every day. This causes IT teams to drown in meaningless malware alerts, try to sort through them, and find the needle in the haystack (Damballa, 2014)[3]. It is practically impossible for even a well-managed IT team to follow up and verify every malware alert.

Target's historic breach of 2013 is a good example of how a cyberattack could devastate a company if not dealt with timely. According to Damballa (2014), Target's IT specialists received a warning that a malicious software infected the company's network but they didn't act on it for two weeks because it was buried among dozens of other high-priority alerts. During the two weeks, criminals had access to credit card information of about 40 million customers. The security breach lead to at least 90 lawsuits and caused a fall in Target's quarterly profits and stock price.

Oncea data breach occurs,companies are forced to spend large sums of moneyon investigations, notifications, and response. The cost of lost reputation and lost business due to a data breach can hit a company hard as was the case for Target Stores in 2013. Affected companies must spend heavily to regain their reputation, try to keep old customers, and attract new customers.Ponemon Institute (2014) found that the average cost of data breach to a company was about US$3.5 million in 2013, a 15 percent increase from the previous year. The study also found that the average consolidated cost of a data breach was $145 for each lost or stolen record containing sensitive and confidential information. This was a more than 9% increase from the previous year.

[2] IBM is the sponsor of the 2014 Cost of Data Breach Study by Ponemon Institute. The study includes more than 250 organizations from eleven countries: Australia, Brazil, France, Germany, India, Italy, Japan, United Kingdom, UnitedStates and, for the first time, Saudi Arabia and the United Arab Emirates.

[3] Damballa is an Atlanta-based company known for engineering advanced, industry-leading cyber-threat defense solutions since 2006.

The 2013 Ponemon Institute's Global Cost of a Data Breach study showed that the industry that incurred the most cost in 2012 was the Healthcare industry ($233 per lostrecord), followed by the Financial industry ($215per lostrecord), and Pharmaceutical industry ($207per lostrecord). Retail was at the lowest spectrum with data breach cost of $78 per lost record. The average cost per data breach varies across countries due to data protection laws in the respective countries and the typesof attacks and threats that organizations face.The U.S.and Germany continued to incur the most costly data breaches with an average cost per lost record of $188 and $199, respectively. U.S.and Germany also had the highest total cost per data breach $5.4 million for the U.S. and $4.8 million for Germanyin 2012 (Ponemon Institute, 2013)[4].

Costs to the U.S. Government

TheInternal Revenue Service(IRS) loss due tofraudulent tax returnsthat result in fraudulent refundhas a direct negative impact on federal government revenue. According to the Treasury Inspector General for Tax Administration, identity thieves stole in excess of $5.2 billion in fraudulent tax refunds in 2010 (Treasury Inspector General for Tax Administration, 2012).

In addition, CSN (2014) indicated that the most common form of reported identity theft during the calendar year 2013 was government documents/benefits fraud (34%), followed by credit card fraud (17%), phone or utilities fraud (14%), bank fraud (8%), employment-related fraud (6%) and loan fraud (4%).Thirty percent of all the government documents/benefits fraud originated from the misuse of information for taxor wage-related fraud while 2.3% was for government benefits applied for/received. Paying fraudulent benefits to fraudsters is a costly business to the governments.

The Federal government, for instance, should be expected to incur additional costs as a result of combatting identity theft since it must not only institute federal laws to deal with identity theft but also put in place structure to efficiently reinforce these laws. In actuality, government's expenditures related to identity theft is often negligible because the governmenthas been usingits existing infrastructure in the fight against identity theft. For instance, according to the Congressional Budget Office (CBO, 2014), the implementation of S.149: Stop Identity Theft Act of 2013 is expected to have no significant cost to the federal government. Indeed, S. 149 demands that the Department of Justice (DOJ) combat identity theft related to the filing of tax returns by using its existing resources more efficiently.

The enactment of S. 149 is expected to have a direct but insignificant effect on government spending and revenues. Indeed, the DOJ's funding which is currently allocated to the investigation and prosecution of a wide range of criminal activity, including identity theft, is expected to be reallocated as a result of S. 149. It is estimated that such reallocation would not have a significant net cost to the federal government. In addition, the federal government might collect additional fines because those who will be prosecuted and convicted under S. 149 could be subject to criminal fines. The latter are recorded as revenues and are deposited in the Crime Victims Fund for later use. Because of the small number of identity theft cases to be likely affected by S. 149, the resulting additional revenues and direct spending would not be that significant.

V. Information Breach in a Medical Organization

Types of Information Breaches

The exposure of a large organization like a major healthcare system to data security breach is enormous. There are hundreds of touch points in a single hospital where patient information can be accessedin addition to computer terminals. Since all processes are computer driven, everything from taking an EKG to a doctor noting patient care information on handheld devices such as tablets can be potential sources of an information breach. At the healthcare organization under discussionhere, there are about 20,000 workers that have access to varying amounts of patient information based on the justifiable need associated with their job. Some examples of workers that come into contact with patients' medical information include the staff of hospitals, physician offices, ambulance companies, radiology centers, third party billing companies, and the list goes on.

The following are examples of types of information breaches that were the focus of the consulting engagement:The "Opportunisticinfo breach" where open unattended display screenson computers or other equipmentcan leave the patient information available for opportunistic thieves or snoopers to see and copy.

The"Nosey Employee info breach" where employees who havethe ability to browse medical information, could discuss patients' medical history with others. Nosey employees are a problem in addition to identity thieves because they can potentially discuss patients' drug problems, mental health issues, or sexually transmitted disease infection and create problems for the organization. Story after story was recounted by personnel tasked with investigating potential breaches. Simple privacy is a huge part of people's expectation in

[4] The Ponemon Institute study analyzed data breach experiences from about 300 companies in nine countries and sixteen industries worldwide and included cost by industry.

life. The right to keep information private and only release what you want people to know is fundamental to all of our lives. Privacy policies, education, and monitoring are necessary to ensure that a pervasive ethical culture of privacy exists around people's medical information. .

In addition, bored employees in a healthcare system may start thinking of people they know and checkout their medical file just for some voyeurism to pass the time. This includes co-workers, ex-spouses, and grown children among others. The urge to know if your son's future wife has any history of mental health or drug problems as well as sexually transmitted diseases can be stronger than the ethical constraints one has. In many cases the violation may be less obvious such as in the cases of adult children, and those accessing the information in this way may not even be aware that what they are doing is against the law and unethical.

The "Employee Theft info breach"where thieves among employees are looking to steal information they can use to open credit card accounts, create fake Medicare invoices, and file false tax returns or steal personal information about famous people that might have some value in the tabloid marketplace or for blackmail purposes. A current trend is to get accomplices hired into external healthcare provider offices, which is much easier than getting hired directly on a hospital's staff. Once in a doctor's office that is part of the healthcare system, they often have the same access to information as hospital personnel. The potential for profit is so high that data thieves will pull out all the stops to gain access to people's private information. Every time one system's vulnerability is plugged, thieves modify their strategy and find or create another weak point in the system.

Organizational Responses to the Threat of Information Breaches

Few alternatives were envisioned to deal with the threat of information breachesfor the healthcare organization in question. A four-pronged approach was embarked uponin an attempt to prevent data breaches and protect the organization from exposure to liability from a breach. First,the compliance department was expanded to take the lead on ensuring that all laws and regulations about protection of privacy are being met and to institute policies, procedures, and system changes necessary to maximize the protection of people's PID and health information.

Second, an education effort was initiated to make sure all employees understand the critical nature of following all applicable regulations and the dire consequences of information breaches. As with any new issue that appears for the first time, organizations are going to be unprepared to deal with it initially. They couldn't foresee that leaving patient information open on a screen in a hospital,mightcause it to be stolen by staff or outsiders passing by with a smart phone. Employees are now made aware of such risks and are trained to clear screens before they walk away from a computer. Steps were taken in an attempt to keep privacy awareness high and effect a culture change in the organization. For instance, each time employees log into their computers a splash screen pops up with a message regarding the importance of keeping patient information private and the penalties for not doing so.

Third, access restriction was established to limit employees' access to sensitive information. Employees are now being prevented from having access to entire systems or sections of a system without a bona fide business need for such access. The compliance department was able to significantly reduce risk by identifying groups and individuals that could have their access to sensitive information removed without any impact to their ability to perform their jobs.

Fourth, an electronic monitoring program was established to provide audit trails for access to any system that contains patients' PID. This is expected to help with data breach prevention, the prosecution of offenders, and the ability to answer patient inquiries about their information access history.A large organization such as this one can have hundreds of different systems that must be checked to identify what information is available to those with access to it. A priority list of systems was generated based on exposure risk and on the number of people having access to the various systems.

Ten of the largest applications were identified for the first phase of auditing. This is where things begin to get interesting because many applications were created years ago when producing logs as an activity was never envisioned as something these applications needed to do. If a company that created an application is still in business and still able to modify the application or build some adjunct functionality, modifications were performed to produce logs that track those who had accessed terminals, what screens they looked at, and how long they looked at them. No audit was done in cases where applications couldn't be modified.

With all of the unknowns regarding how much logging was going to be available during the audit, capacity planning for storage was a shot in the dark. Additional storage capacity had to be added multiple times. In some cases 13 million records per day were being generated for just one application.Specific reporting was done on individual activity ranking as well as deviation from "normal" behavior as determined by descriptive statistics such as median and mode. For example if the vast majority of users access a particular terminal screen for about 2 minutes but a certain individual showed a recent pattern of looking at the same screen multiple times for successive patients for only 5 seconds, then such anomalous behavior would stand out for further scrutiny.

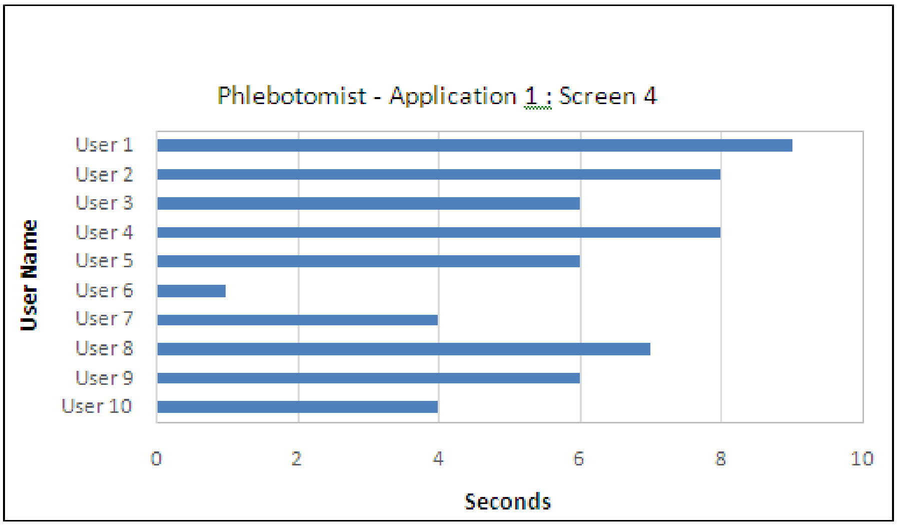
Additional types of audit reporting were also implemented. First, to flag anomalous behavior and activity consistent with mass information theft, the top 10 users in terms of the number of screens accessed and the number of patient records accessed had to be identifiedas shown in Figures 1 and 2.

Figure 1 showsthe median time a particular health worker, a phlebotomist, spent on a particular screen in a particular application or device. Since time spent on the screens of devices will vary by device, software application, and the tasks being performed by a variety of health workers; statistics must be kept at the lowest level of granularity of the device or application and the job function being performed. Anomalies such as User 6 who took only one fifth the time of the others shown indicate a situation that should be investigated. Such a short time is likely too short to do any meaningful work, but long enough to snap a picture of patient information using a cell phone camera.

Figure 2 shows 10 health workers and the number of patients each accessed on a given day. Anomalies such as User 7 who looked at 5 times more records than the others indicate a situation that should be investigated. When the institution in this study retroactively looked at the data at the time of a known breach, the number of patient records accessed by the offender was found to be many multiple times higher than that of other workers.

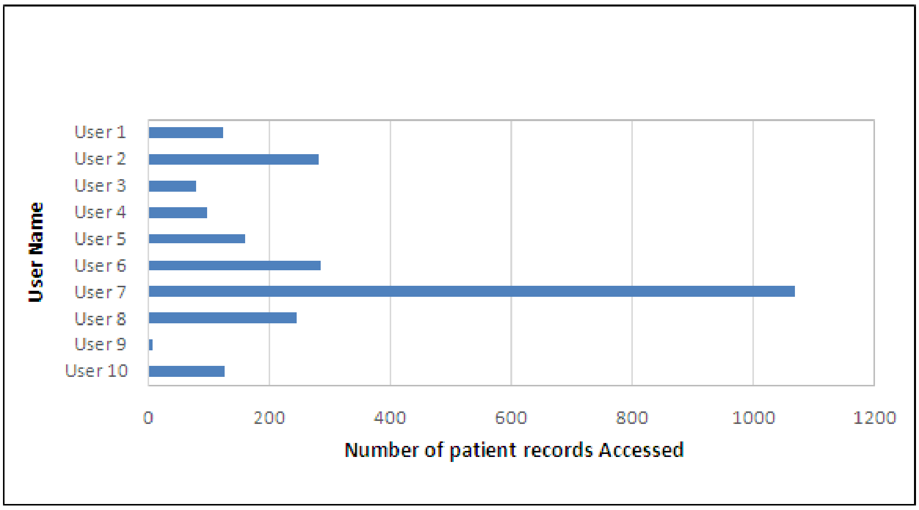
Second, individuals are flagged if they look at the records of other employees working in the same department as them. This identifies potential snooping by coworkers. Third, if a patient is over 70 years old and access of their records is not associated with some recent visit, a flag will be raised. This identifies potential identity theft for tax or Medicare fraud.

Figure 1: Users' Daily Median Time per Screen



Source: Author

Figure 2: Patient Records Accessed in aDay



Source: Author

Fourth, if a patient has been deceased for some time and their records are accessed a flag will also be raised. Finally, if a patient is a VIP such as an executive in the organization or other individuals placed on the VIP list and their records are accessed, a flag will be raised. This identifies voyeurs or paparazzi type activity.The audit system was tested through aretroactive review of historical access activitiesaround the time of known breaches. The nefarious activity stood out like a sore thumb as unusually excessive numbers of screen views were observed during that time.

VI. Conclusion

Data security breaches that could lead to identity theft are occurring at a higher pace as computer network systems become more and more vulnerable from attacks by hackers and viruses.The number of consumer victims of identity theft has also been rising over the years, from about 8.3 million U.S. adults' victimsin 2005 to 13.1 million victims in 2013. The dollar amount stolen from identity fraud rose from about 15.6 in 2005 to about $18 billion in 2013.Even thoughmost victims of identity theft do not incur any out of pocket expenses, they all incur indirect costs such as cost of having bad credit and the opportunity costs associated with time spent resolving issues resulting from their information being stolen.

Businesses have been incurring increasingly higher cost from data breaches. The average cost of data breach to a company was about US$3.5 million in 2013, anincreaseof 15 percent from 2012.The U.S. federal government is also not immune from the costs of identity theft, as identity thieves use stolen identity for tax fraud and othergovernment documents\benefits fraud.Consequently, governments and private organizations are responding to the threat of data security breaches and information theft through laws, stronger security systems, and monitoring services but identity thieves find ways to circumvent it all. Identity thieves have become more and more creative and will not stop their activities as long as there is a substantial economic benefit and a fairly low chance of getting caught.

For a healthcare network system or any organization with a network system, limiting information access only to employees with a bone fide business reason is a good start to data-breach prevention. Training in ethics and responsible handling of people's electronic and other information is another important component of a good information management policy. Electronic monitoring of access activity is a critical piece to ensure that breaches are detected as soon as possible and information releases can be prevented, stopped, or minimized.

This study recommendsthatthe use of SSN for medical identification be eliminated and replaced with a unique identifier specifically for medical use.The latter approach could also be implemented in other industries that convenientlyuse SSN, which virtually every American has memorized, for identification purposes. In fact, the use of SSN in employment or credit mattersdoes not necessarily provide verification that the person using it is the individual whom it identifies. Consequently, SSN is easily used by criminals to impersonate people and engage in a variety of fraud.

For people on Medicare,the Medicare Number; which is used for their medical transactions, shouldalso be used as an identifying number rather than the SSN. All references to SSN should then be purged from their electronic information. For everyone else, an alternate Medical Number should be generated and used instead of SSN and that SSN be purged from the electronic file of everyone. Thismay occur over time as we creep toward a single payer government system.

Organizations should employ better encryption and robust authentication methods and employees must be educated and trained on how to handle sensitive and confidential information. Cyber insurance could play an important role not only in managing the risk of a data breach but also in enhancing the security position of the company. However, insurance could encourage a company to slack off on cyber security. This is a moral hazard that should not be overlooked.

Finally, an efficient response to a breach and containment of the damage could significantly diminish the cost of breach. Thus, companies should consider having an incident response and crisis management plan in place as a preventive measure to data breach and damage control when one occurs. Note that the organizational responses to the threat of data breaches examined in this paperare equally applicable to any organization that needs to protect people's PID.

References

[1]. Acohido,B. "Analysis: Why LivingSocial disclosed huge data theft," USA Today, 2013. Retrieved from

[2]. http://www.usatoday.com/story/tech/2013/04/30/livingsocial-50-million-accounts-breached-cybersecurity-privacy-invasion/2124345/

[3]. Anderson, K.B., E. Durbin, and M.A. Salinger. "Identity Theft," Journal of EconomicPerspectives,22,2008, 171-192.

[4]. Anderson, K.B. "Who Are the Victims of Identity Theft? The Effect of Demographics." Journal of Public Policy & Marketing,25(2), 2006, 160-71.

[5]. Cardenas, H."Jump drive Abuse in the Workplace."Houston Chronicle, 2013.Retrieved from http://work.chron.com/jumpdrive-abuse-workplace-20317.html.

[6]. Cheney, J. "Identity Theft: Do Definitions Still Matter?" Federal Reserve Bank of Philadelphia Payment Cards CenterDiscussion Paper, 2005.

[7]. Consumer Sentinel Network (CSN). “Data Book.”Federal Trade Commission, 2014. Retrieved from

[8]. http://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-january-december-2013/sentinel-cy2013.pdf.

[9]. Congressional Budget Office (CBO).“S.149, Stop Identity Theft Act of 2013: Cost Estimate,”2014. Retrieved from http://www.cbo.gov/publication/45172.

[10]. Damballa.“Cyber Defense: Cut Through the Noise, Bloomberg Businessweek,” May 26-June1, 2014.

[11]. Department of Health and Human Services (DHHS). “New rule protects patient privacy, secures health information,"2013.Retrieved from http://www.hhs.gov/news/press/2013pres/01/20130117b.html.

[12]. Federal Trade Commission (FTC). “Identity Theft and Assumption Deterrence Act,” 1998.Retrieved from http://www.ftcgov/node/119459.

[13]. _______. “Consumer Fraud and Identity Theft Complaints: January-December 2005,” 2006.Retrieved from http://www.consumer.gov/sentinel/pubs/Top10Fraud2005.pdf

[14]. _______.“Identity Theft Red Flags and Address Discrepancies under the Fair and Accurate Credit Transactions Act of 2003: Final Rule,” 2007. Retrieved from http://www.gpo.gov/fdsys/pkg/FR-2007-11-09/html/07-5453.htm

[15]. _______. “Fair Credit Reporting Act 15 U.S.C. § 1681,”2012.Retrieved from http://www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0111-fair-credit-reporting-act.pdf

[16]. Javelin.“Strategy & Research Study,”2014.Retrieved fromhttps://www.javelinstrategy.com/news/1467/92/A-New-Identity-Fraud-Victim-Every-Two-Seconds-in-2013-According-to-Latest-Javelin-Strategy-Resea rch-Study.

[17]. Jewell, M. “Groups: Record Data Breaches in 2007.” Associate Press, 2008.Retrieved from http://attrition.org/news/content/08-01-03.001.html.

[18]. Kahn, C. and W.Roberds. “Credit and Identity Theft.” Federal Reserve Bank of Atlanta Working Paper No 19, 2005.

[19]. Lai, F., D. Li, and Chang-Tseh Hsieh.“Fighting Identity Theft: The Coping Perspective.”Decision Support Systems, 52(2),2012,353-363.

[20]. McCann, E.“Top 10 Healthcare Breaches of 2012,” 2012. Retrieved fromhttp://www.healthcareitnews.com/news/infographic-biggest-healthcare-data-breaches-2012

[21]. Ponemon Institute. “2013 Cost of Data Breach Study: Global Analysis,” 2013. Retrieved from http://www.ponemon.org/local/upload/file/2013%20Report%20GLOBAL%20CODB%20FINAL%205-2.pdf

[22]. ______. “2014 Cost of Data Breach Study: Global Analysis,” sponsored by IBM, 2014. Retrieved from http://www.ponemon.org/blog/ponemon-institute-releases-2014-cost-of-data-breach-global-analysis.

[23]. Treasury Inspector General for Tax Administration. “There are Billions of Dollars in Undetected Tax Refund Fraud Resulting from Identity Theft,”2012. Retrieved from http://www.treasury.gov/tigta/auditreports/2012reports/201242080fr.pdf

[24]. Roberds, W. and S. L. Schreft. “Data Breaches and Identity Theft.” Journal of Monetary Economics,56(7),2009, 918-929.

[25]. Schreft, S. L. “Risks of Identity Theft: Can the Market Protect the Payment System?”

[26]. Federal Reserve Bank of Kansas City Economic Review, Fourth Quarter, 2007, 5-40.

[27]. Solove, D. “The New Vulnerability: Data Security and Personal Information,” in Securing Privacy in the Internet Age, Radin&Chander, eds.,Stanford University Press, 2008.

[28]. Synovate.“Federal Trade Commission—2006 Identity Theft Survey Report.”McLean, VA, 2007. Retrieved from www.ftc.gov/os/2007/11/SynovateFinalReportIDTheft2006.pdf.