Passwords Selected by Hospital Employees: An Investigative Study

B. Dawn Medlin
Computer Information Systems
Appalachian State University
Boone, NC, USA

Ken Corley
Computer Information Systems
Appalachian State University
Boone, NC, USA

B. Adriana Romaniello
Economía de la Empresa
Universidad Rey Juan Carlos
Madrid, Spain

Abstract— **The health care industry has benefitted from its employees' ability to view patient data, but at the same time this access allows for patient's health care records and information to be easily tampered with or stolen. Access to and transmission of patient data may improve care, increase delivery time of services and reduce health care costs, security of that information may be jeopardized due to the innocent sharing of personal and non-personal data with the wrong person. In this study, we surveyed employees of different size hospitals in various regions of the state who were willing to share their passwords. Our findings indicate that employees need further or additional training in their awareness surrounding password creation.**

Keywords- Passwords; Security; HIPPA; HITECH.

I. INTRODUCTION

Health care records generally include, but are not necessarily limited to, individual patient's health history, diagnosis, laboratory results, treatments, and the doctor's progress notes. A patient's personal information, such as address, phone number, and social security number, are all items that may be included and accessible to some or all health care employees. These records are vulnerable to security breaches and theft. Both hackers and social engineers have successfully found ways to penetrate networked health data systems by simply asking for the information or by finding weaknesses within the system.

Unfortunately, the largest threat to a health care agency's security may not be outsiders, but rather their own employees. Inside employees actually can pose the largest threat to the security and privacy of information as they can exploit the trust of their co-workers, and they generally are the individuals who have or have had authorized access to the organization's network and who are familiar with its internal policies, procedures, and technologies. Additionally, internal employees can exploit that knowledge to facilitate attacks and even collude with external attackers (Insider Threat Research). Due to increased regulations and the increased opportunities for exploitation that exist in today's digital world, it is even more important for health care providers to keep health care records and the information held within, safe and private. Governmental agencies have adopted initiatives that specifically address the issues and rights of health care patients. More specifically, the security and privacy of health care information is protected by HITECH (Health Information Technology and Clinical Health Act) and the Health Insurance Portability and Accountability Act (HIPAA), requiring health care agencies to do everything possible to protect their information.

II. BACKGROUND

The electronic accumulation and exchange of personal health information has been promoted as a significant benefit to health care consumers and providers. Many health care policy experts believe that broader health information technology adoption may lead to the availability of more complete and transparent information, ultimately helping to contain health care costs while simultaneously improving health care quality.

Managers must be vigilant in their efforts to protect patient information as required by several laws. On February 17th, 2009, President Obama signed into law the Health Information Technology and Clinical Health Act (HITECH) as part of the American Recovery and Reinvestment Act. The HITECH Act enhances the security and privacy provisions as well as the penalties contained in the Health Insurance Portability and Accountability Act of 1996 (The Health Information Technology for

Economic and Clinical Health Act (HITECH Act): implications for the adoption of health information technology, HIPAA, and privacy and security issues, 2009). This new law also requires patients be notified in the event of a security breach.

In addition to HITECH, the basic goal of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) is to protect the privacy and security of patients and their medical records. Furthermore, HIPAA addresses security and privacy measures in relation to passwords, either directly or indirectly, in the following standards: 1) **Security Management Process [161.308(a)(1)]** Health care organizations must show that they have a consistent set of internal processes, with implementation that is widespread and institutionalized. Processes range from establishing criteria for who has access to what, and who can request certain resources; to ensuring that access rights are revoked immediately upon employee termination, 2) **Security Awareness and Training [161.308(a)(5)]** HIPAA requires that staff members be trained and educated concerning the proper handling of PHI. This basic-level security training should include measures such as password management, and 3) **Access Control [161.312(a)]** HIPAA security regulations require a definition of who has access to PHI within the organization, as well as the rules determining an individual's right of access, and the reasons for denying access to some individuals.

Despite its legal requirements, however, HIPAA standards are not always followed. As an example, a public posting of 20,000 emergency room patients who had visited Stanford Hospital in Palo Alto, California, was placed on a commercial Web site that included the patient's names and diagnosis codes. The hospital confirmed that the information remained online for nearly a year (Sack, 2011). Another example included a laptop that was stolen from a rehabilitation center containing 660 patient's records. The laptop which was reported stolen from Rancho Los Amigos National Rehabilitation Center on Feb. 24, 2011 contained at least 667 patient names, their date of birth and diagnostic information (Downey, 2011). These are only two examples of some of the thousands of medical records that are either stolen or lost each year.

The Federal Trade Commission (FTC) and the Department of Health and Human Services (HSS) in 2009 issued the first set of HIPAA privacy/security guidance under the new HITECH Act requirements. The new guidance relates to the security breach notification requirement, that states "Under this requirement, health plans and personal health record (PHR) vendors must provide individual notification if there has been a security breach of protected health information" (http://compliance.utimaco.com/na/tag/hitech- act/).

Additionally, notification must be provided to individuals in writing within 60 days of discovery of the breach. If the breach involves more than 500 individuals, notice also must be made in prominent media outlets and to the Secretary of Housing and Health Services or to the FTC for PHR vendors (Health IT Data Breaches: No Harm, No Foul).

For health care administrators, security is enhanced by using systems tools that are already available, such as Active Directory and LDAP **(**Lightweight Directory Access Protocol)**.** Most likely, one or the other, or a combination of both is already in use to help in the securing of information. Even when other front-end access management products, like IBM Tivoli, Citrix or Sun Microsystems' Java System Identity Manager are in use, the directory server on the back end is likely to be Active Directory, LDAP or both.

In addition, more health care agencies may consider adopting biometrics. Biometrics is the science of identifying people through physical characteristics. Usually not one technology but a cluster of several, biometrics uses fingerprints, handprints, retina scans, voice recognition, facial structure, and even hand motions while writing a signature-to identify individuals (Simpson, 2002).

Smart cards may also be used as these operate with a chip that includes stored memory, and an operating system. A patient's entire clinical history is stored on the smart card which can only be accessed via reading devices in a physician's office, primary care center, hospital, or other medical institution. Through the use of this device, exposed paper records will not be a concern. An added benefit of smart cards is the ability for users to electronically forward patient information to other health care authorities and insurers. Specifically, Java-based card technology emerges as a leading platform because of its ability to support multiple health care applications securely, while incorporating biometrics for positive identification and authentication.

A. Issues

Americans hold a strong belief in their right to privacy, and that belief has been served by the legal system of the United States. Privacy is also a constitutional concept, as found in the Fourth Amendment to the U.S. Constitution (Gostin, 2000). In fact, the preamble to the federal Privacy Rule, promulgated pursuant to HIPAA, notes that the existence of a generalized right to privacy as a matter of constitutional law suggests there are enduing values in American law related to privacy.

As required by HIPAA as well as other state laws, health care institutions are required to provide security methods in order to protect patient's information. One such method is through the authentication of the individual requesting access. Health care employees are generally subjected to some type of authentication process. Although there are different ways of authenticating employees, most systems are based on the use of a physical token (something one has), secret knowledge (something one knows) or biometrics (something one is) (Burnett & Kleiman, 2006).

In today's health care institutions, the most common authentication mechanism is still the simple use of a password (something one knows or creates). This type of authentication method can offer to employees the ability to quickly enter into a system, but human practices such as using the same password on different systems and writing down a password may degrade the quality of password security (Pfleeger and Pfleeger, 2007).

The authentication method of individuals creating their own passwords is not atypical. For health care organizations the password functions like the key to a lock, anyone who has it can get in to see the patient's information. Toward that end, there have been recommendations from governmental agencies to hospitals on how to construct a password. One of the first guidelines in creating good passwords was published in 1985 by the Department of Defense and is still relevant today (Department of Defense. 1985). Their guidelines recommended the following: 1) passwords must be memorized; 2) passwords must be at least six characters long, 3) passwords must be replaced periodically, and 4) passwords must contain a mixture of letters (both upper- and lowercase), numbers, and punctuation characters.

Most networks administrators and security experts would concur with all of the above Department of Defense recommendations, however, that was in 1985 when the advice was given and when social engineering as well as other types of attacks were not as common as they are today. According to CERT (the Computer Emergency Response Team), the advice to use upper and lower case alpha characters for Novell and/or VMS systems is useless since both of these systems are case insensitive.

B. Problems

Many of the deficiencies of password authentication systems arise from the limitations of human cognitive ability (Pond et al., 2000). If humans were not required to remember a password, a maximally secure password would be one with maximum length that could consist of a string of numbers, character, and symbols. In fact, the requirements to remember long and complicated passwords are contrary to the way the human memory functions. First, the capacity of human memory in its capacity to remember a sequence of items is temporally limited, with a short-term capacity of around seven items plus or minus two (Kanaley, R., 2001). Second, when humans remember a sequence of items, those items cannot be drawn from an arbitrary and unfamiliar rang, but must be familiar 'chunks' such as words familiar symbols. Third, the human memory thrives on redundancy.

In fact, studies have shown that individuals' short term memory will retain a password for approximately 30 seconds thereby requiring individuals to attempt to immediately memorize their passwords. It has also been shown that if an individual is interrupted before they fully memorize the password; it will fall out of their working memory and most likely be lost.

Also, if an individual is in a hurry when the system demands a new password, individuals must sacrifice either the concentration of the critical task at hand or the recollection of the new password. Related to this issue is having to create the content for this new quickly demanded password. The pressure to choose creative and secure passwords quickly generally results in individuals failing in their attempt to memorize this new password. For health care organizations this can result in reset rates at one per reset per every four to five users per month (Brostoff and Sasse, 2001).

In order to combat the issue of having to remember so many different passwords some users have resorted to the selecting familiar terms such as a pet or family name, their own name, their phone number, or other common terms that could be found in a dictionary. British psychologist Helen Petrie, Ph.D., a professor of human/computer interaction at City University in London analyzed the passwords of 1,200 British office workers who participated in a survey funded by CentralNic, an Internet domain-name company in 2001. She found that most individuals' passwords fell into one of four distinct password categories which were family, fan, fantasists, and cryptic.

The first category of "family," comprised nearly half of the respondents. These individuals selected their own name, the name of a child, partner or pet, birth date, or significant number such as a social security number. Further, Dr. Petrie found that individuals also choose passwords that symbolized people or events with emotional value or ties.

One third of the survey participants were identified as "fans," using the names of athletes, singers, movie stars, fictional characters, or sports teams. Dr. Petrie also found that these individuals wanted to align themselves with the lifestyle represented by or surrounded around a celebrity status. Two of the most popular names were Madonna and Homer Simpson.

Fantasists made up eleven percent of survey responses. Dr. Petrie found that their passwords were comprised of sexual terms or topics. Some examples included in this category were terms such as "sexy," "stud" and "goddess."

The final ten percent of participants were identified as "cryptics." These users were seemingly the most security-conscious, but it should also be noted that they were also the smallest of all of the four identified categories. These individuals selected unintelligible passwords that included a random string of letters, numerals, and symbols such as Jxa+157.

Self-created computer passwords are generally personal, and they reflect the personalities of millions of people as they attempt to summarize their life through a few taps on the keyboard. As psychologists know, people and personalities are often very predictable in the aggregate (Andrews, 2004), as may be their choices of passwords. Psychologists have found that humans can store only five to nine random bits of information in their short-term memory, making it difficult to remember long and complicated passwords. Therefore, users have often chosen passwords with personal meanings that they can associate with something in their long-term memory.

III. RESEARCH METHODOLOGY

A. Data Collection

To obtain a fair statistical representation of the password security used in relation to health care organizations, a survey was given to employees at five hospitals of various sizes and in different regions of the state. Hospital administration approval was obtained, but the administration did not endorse the survey to respondents, nor did they ask them to participate. The data set was comprised of 118 responses. Data was gathered to not only determine how many employees would disclose their passwords and other personal information such as their address, phone number and email, but also simulated the types of information individuals were willing to share with co-workers, colleagues, or friends of colleagues. The information that employees were willing to share, including their passwords and other personal information, would certainly make it easier to hack into a system instead of having to "guess" at the necessary authentication information.

B. Analysis and Results

As seen in Table 1 (labeled password categories), half of the respondents created passwords consisting of family names, including their own name or nickname, the name of a child, or significant other. Interestingly, the findings noted in Table 2 indicate that most respondents were often required to use a password to access systems, but rarely changed their passwords. As further indicated, most of the respondents used the same password on multiple accounts. The practice of rarely changing passwords and/or using the same password for multiple accounts would assist social engineers, thus allowing them to easily attain access to one system and possibly more.

TABLE 1. PASSWORD CATEGORIES

Variable Name	Question	Answers	N	Mean	Std Dev
Family	Does your password fit into this category?	1 = Yes, 0 = No	118	0.50	0.50
Cryptic	Does your password fit into this category?	1 = Yes, 0 = No	118	0.05	0.22
Number	Does your password fit into this category?	1 = Yes, 0 = No	118	0.45	0.50
Fan	Does your password fit into this category?	1 = Yes, 0 = No	118	0.15	0.95
Faith	Does your password fit into this category?	1 = Yes, 0 = No	118	0.03	0.18
School	Does your password fit into this category?	1 = Yes, 0 = No	118	0.02	0.13
Fantasy	Does your password fit into this category?	1 = Yes, 0 = No	118	0.00	0.00
Place	Does your password fit into this category?	1 = Yes, 0 = No	118	0.14	0.34
Other	Does your password fit into this category?	1 = Yes, 0 = No	118	0.51	0.50

Additionally, as seen above in Table 1, the largest category of password choices included some type of relationship to a family name being reported at fifty percent (50%). Fifteen percent (15%) of the respondents self-reported the inclusion of "fan-based" words, which could include names of athletes, singers, movie stars, and fictional characters or sports teams. "Place" was the next highest category, with fourteen percent (14%), using another identifiable piece of information such as the city where the employee works/lives.

The smallest of all of the self-identified password categories was "fantasy," followed closely by the categories of school and faith. Five percent (5%) of the employees selected the "cryptic" category, suggesting that these employees are security-conscious since that category includes passwords that are unintelligible.

TABLE 2. PASSWORD STATISTICS

Variable Name	Question	Answers	N	Mean	Std Dev
Pass_Freq	How often do use a password to access systems?	1= Very Often 5= Never	118	1.23	0.59
Pass_ Change	How often do you change your passwords?	1= Very Often 5= Never	117	2.85	1.13
Reuse	Most people use the same password on multiple accounts. How often do you do this?	1= Very Often 5= Never	118	2.47	1.32

As noted in Table 3, in the area of password and security training, most of the respondents, fifty-four percent (54%) indicated that their employer had offered password security training, with fifty-eight percent (58%) of the hospitals offering some other type of security awareness training (Table 3). Attendance by the employee in either a current password or security awareness training program was measured on a Likert scale of 1 being last week and 5 being never. The employees indicated that currently, they almost never attended the security awareness programs.

TABLE 3: PASSWORD TRAINING

VAR NAME	QUESTION	ANSWER	NO	MEAN	STD DEV
Pass_Train	Does your employer offer password security training?	1 = Yes, 0 = No	115	0.54	0.50
Awar_Train	Does your employer offer any other security awareness training?	1 = Yes, 0 = No	113	0.58	0.50
Current_Train	When was the last time you participated in either a password or another security awareness training program?	1= Last week, 5 = Never	115	4.09	1.08

IV. DISCUSSION

This study reveals several interesting findings. As noted earlier, most employees used the same passwords on multiple accounts, even though they frequently changed them. The actions of repeatedly using the same password are contrary to suggested recommendations by most security experts, because a hacker who gained access to one account could more easily access other systems. Requiring individuals to maintain a new password for each system or application would obviously make systems more secure but is in conflict with humans' short-term human memory capabilities. Employees may consider it necessary to include familiar names, places, and numbers in their passwords so that they can easily recall them.

Though most employees indicated that their employers offered password security training either very often or often, it appears that either the types of training are not very effective or that the employees did not take it very seriously.

V. CONCLUSION

Findings of the present study indicate that employees are willing to share personal information with co-workers and friends of co-workers. Seventy-three percent (73%) of the employees shared information that a social engineer could use to create a profile of an employee and gain access to the employer's network and other confidential patient information. It is imperative that employees understand the consequences of sharing information as well as the importance of creating and maintaining strong passwords.

The simulation that was carried out during this study demonstrated that many employees may currently be in violation of HIPAA and HITECH regulations due to their willingness to share their information and their practice of creating weak passwords, thus allowing for easy access into a system. Hospitals and other health care agencies must identify ways to educate employees regarding HIPAA and HITECH regulations to protect patients and practices to create a long password, but on the other hand offers it freely to others. This study demonstrated that many employees may currently be in violation of HIPPA and HITECH regulations due to their willingness to create weak passwords and to share them with strangers through our survey instrument.

REFERENCES

[1] 6 Password Protection Tips That Every Computer User MUST Know!. Retrieved on October 23, 2011 from http://www.richtechgroup.com/business/2011/04/6-password-protection-tips-that-every-computer-user-must-know/

[2] Andrews, L.W. (2004). Passwords reveal your personality. Retrieved March 13, 2007, from http://cms.psychologytoday.com/articles/pto-20020101-000006.html.

[3] Brostoff, S., & Sasse, M. A. (2001). *Safe and Sound: a safety-critical approach to security*. Position paper presented at the New Security Paradigms Workshop 2001, Cloudcroft, New Mexico. [4] Burnett, M. & Kleiman, D. (2006). *Perfect Passwords. Selection, Protection, Authentication.* Syngress.

[5] Data Breach Harm Analysis from ID Analytics Uncovers New Patterns of Misuse Arising from Breaches of Identity Data. Retrieved on November 12, 2009, http://www.idanalytics.com/news_and_events/20071107.html

[6] Department of Defense. (1985). Password Management Guideline. http://www.alw.nih.gov/Security/FIRST/papers/password/dodpwman.txt

[7] Downey (2011). Laptop Stolen from Rehab Center with Over 660 Patient Records. KTLA News. Retrieved on October 23, 2011 from http://www.ktla.com/news/landing/ktla-laptop-stolen-from-downey-rehab,0,3270396.story

[8] Georgetown University Information Security. Retrieved November 12, 2009, from

[9] Gostin, L.O. (2000). Public Health Law: Power, Duty, Restraint. University of California Press , Berkeley, CA. pp. 132-134.

[10] Gragg, D. (2007). A Multi-Level Defense Against Social Engineering." SANS. http://www.sans.org/reading_room/whitepapers/engineering/920.php.

Human Memory. Intelegen, Inc. Retrieved on December 1, 2009 from http://brain.web-us.com/memory/human_memory.htm.

[11] Health Law Alert. Retrieved on November 15, 2009 from http://www.nixonpeabody.com/publications_detail3.asp?ID=2621.

[12] Health IT Data Breaches: No Harm, No Foul. Retrieved on Novemer 12, 2009 from http://compliance.utimaco.com/na/tag/hitech-act.

[13] Hupp, M. (2007). Protecting patient medical records from the nosy. Retrieved on November 30, 2009 from http://www.bizjournals.com/milwaukee/stories/2007/11/12/focus3.html?t=printable.

[14] Insider Threat Research. Retrieved December 1, 2009 from http://www.cert.org/insider_threat.

[15] Internet Identity Theft And Password Security Tips. Retrieved on October 23, 2011 from http://www.combat-identity-theft.com/internet-identity-theft.html

[16] Kanaley, R. (2001). Login error trouble keeping track of all your sign-ons? Here's a place to keep your electronic keys, but you better remember the password. *San Jose Mercury News*, 3G.

[17] Pfleeger, C.P. & Pfleeger, S.L. (2007). *Security in Computing*. Fourth edition. Prentice Hall.

[18] Pond, R., Podd, J., Bunnell, J., Henderson, R. (2000). "Word Association Computer Passwords: The Effect of Formulation Techniques on Recall and Guessing Rates," *Computers & Security*, 19, 645-656.

[19] PROTECTING HEALTH INFORMATION. RETRIEVED ON NOVEMBER 12, 2009 FROM HTTP://WWW.HHS.GOV/NEWS/FACTS/PRIVACY.HTML.

[20] Sack, K. (2011). Patient Data Posted Online in Major Breach of Privacy. New York Times. Retrieved on October 23, 2011 http://www.nytimes.com/2011/09/09/us/09breach.html?pagewanted=all)

[21] *Simpson*, R.L. (2002). Nursing Management. Chicago: 33(12), 46-48.

[22] The Health Information Technology for Economic and Clinical Health Act (2009). Retrieved on October 23, 2011 from http://www.nixonpeabody.com/publications_detail3.asp?ID=2621

[23] Thompson, S. T. Helping the Hacker? (2006) Library Information, Security, and Social Engineering. Information Technology and Libraries. Chicago: 25(4), 222-226.

AUTHORS PROFILE

B. Dawn Medlin is the Chair and Professor in the Department of Computer Information Systems and the Co-Director of the Center for Advanced Research on Emerging Technologies, John A. Walker College of Business, at Appalachian State University in Boone, NC. During her 24 years of teaching she has taught courses such as Web 2.0 Technologies in Business, Introduction to Gaming, Advanced Security, Issues in E-Commerce, She has published in journals such as The Journal of Information Systems Security, Information Systems Security, International Journal of Electronic Marketing and Retailing, and the International Journal of Healthcare Information Systems and Informatics. Additionally, she has taught at the Université d'Angers and Addis Ababa University in Ethiopia.

Ken Corley is an Assistant Professor of Computer Information Systems at Appalachian State University. He received his Ph.D. from Auburn University in Auburn, Alabama, USA. His current research interests include information privacy & security, computer and human interaction, and sustainability.

B. Adriana Romaniello, originally from Uruguay, is an Interim Associate Professor of Management at the Department of Business Administration at University Rey Juan Carlos (Madrid, Spain) who came from University Carlos III (Madrid) where she teaches Corporate finance. She holds a Ph. D. in Business Administration at University Complutense of Madrid and a Licentiate degree in economics and business from University of La Republica (Uruguay). She teaches management, organization theory and organizational design to undergrads and doctoral students. Adriana's research interests focus on information security, organization theory and competitive strategy.