https://doi.org/10.48009/1_iis_2016_178-184

A SURVEY OF SOCIAL ENGINEERING VULNERABILITIES IN HEALTH CARE SETTINGS

Sushma Mishra, Robert Morris University, mishra@rmu.edu
Peter Draus, Robert Morris University, draus@rmu.edu
Natalya Goreva, Robert Morris University, goreva@rmu.edu
Don .J. Caputo, Robert Morris University, caputo@rmu.edu

ABSTRACT

The major thrust and direction of this study is an examination of the increasing encroachment of technological and social forces into the fabric of the medical healthcare facilities that comprise the entirety of the U.S. Health Care System. The new initiatives, formally promulgated by the HIPAA regulatory structure, includes security, privacy, transparency, awareness, perceptions and assessments of threats, and training as the response to social engineering incursions. The demographics for the study were obtained through a survey instrument that examined and interpreted multiple categories of responses, such as age, employment experience, education, work category, gender, facility size, access-standards and computerization level. Training, personal device usage and access control measures comprise the three areas designated as research questions. They are statistically resolved and interpreted, with conclusions drawn and future related directions provided.

Keywords: Social Engineering, Survey, Mobile Devices, Access Control, Training, ANOVA, Correlation

INTRODUCTION

Comprehensive security planning requires formal, informal and technical controls. The technology alone is not sufficient to mitigate and reduce risk form internal threats in organizations (Anderson and Moore, 2008). Organizational security governance requires development of objectives that incorporate controls addressing threats from insiders in form of social engineering and weave these controls into the overall fabric of security preparedness (Mishra, 2015). Prevention of social engineering threats in the context of healthcare organizations is of prime importance to the viability of an organization since the information leaked in such an attack can be disturbing, damaging, or even dangerous to the extent that legal consequences can ensue for the patient or hospital.

Social Engineering is defined as any act that influences a person to take an action that may or may not be against the best interests of their organization. This is not the same as the more common and more technological brute force methods known widely as computer hacking. Increasingly, it has evolved into a general definition of the incursions of social engineering tactics into the healthcare environment, and specifically the vulnerabilities of the target employee, i.e. the caregiver. Because perception, awareness, and response are crucial elements of any healthcare system, a roadmap detailing the inroads of Social Engineering is constructed. A fundamental question of susceptibility arises in determining how the social engineering threat impacts healthcare workers in terms of access control measures for all levels of members in the organization, access of mobile devices from remote places, and regular staff training to educate employees about persistent recurring issues.

As a precursor to managing the challenges of protecting the healthcare environment from social engineering intrusions, we need first to determine in this study if employees are aware of the meaning and ramifications of Social Engineering, and how much of a threat it presents in their everyday work environment. Then we need to discover how the healthcare employee perceives and responds to procedures and policies within various categories. These categories include job classification, number of years employed in field, clinical or administrative duties, age, gender, academic degrees obtained, training within their field of responsibility, level of computerization within their work setting, size of the healthcare organization, and even a willingness to report existing improper or illegal procedures, also known as “whistle-blowing”. The goal of this study is to understand how healthcare organizations address threats arising from social engineering techniques in the area of access control, mobile devices and training, or lack of training thereof. The specific research questions that this study will address are:

RQ1: How does social engineering practices impact access control measures in health care organizations?

RQ2: How do social engineering techniques impact personal device access issues in healthcare settings?

RQ3: How does management intervention in the form of regular training for employees impact the risk from social engineering threats in healthcare settings?

The remaining of this paper is organized as following. The introduction section is followed by a review of literature in social engineering, impact of mobile devices security threats, access control in healthcare settings and role of training in mitigating risk areas. The methodology section presents data collection and analysis followed in this study by a discussion of the implications of results. Conclusions are drawn.

LITERATURE REVIEW

To the casual observer of systemic computer integration into social movements and structures, the art and science of social engineering is a recent phenomenon that arose only with the introduction of small technological devices such as the laptop, the IPAD and the smartphone, and finally culminating in the introduction of the software that supports them (Malatesti, 2016). On the contrary, the antecedents of social engineering can be traced back nearly 40 years, where it was a nascent attempt to influence or disrupt activities within corporate structures, slowly gravitating to government and institutional entities such as Health Care (Whiteside, 1977). It was known then as “Dead Souls in the Computer.” These early occurrences were characterized by the fact that they were one-dimensional in nature, and generally carried out by insiders in single-stage assaults. Most likely, they were individuals who were insiders within the technological infrastructure of the corporate entity or industry.

The information security process in healthcare has always depended on the effective leadership and the corresponding distribution of security policies among all healthcare workers, particularly focusing on their motivation and training. Healthcare organizations invest large proportions of time and money trying to protect their resources, privacy and security. While enjoying technological successes in their realm, one popular means of gaining access and meaningful information has been somewhat overlooked. Welcome to the emerging world of Social Engineering.

Today, we are witnessing the rise of multifaceted social engineering attacks that have become increasingly sophisticated and able to bypass security initiatives that are designed to prevent any incursions into areas that are demonstrably sensitive to intrusion (Gartner, 2016). Social Engineering within the field of medicine and health care not only serves as a costly threat but, due to the nature of the health care spectrum, a potentially lethal one. Social engineering techniques target natural human attributes that can be exploited for gain. Employees in healthcare settings are constantly interacting with patients and their care providers. As such, they are exposed to social engineering maneuvers targeted at extracting information that is highly privileged and sensitive. Authority, liking, reciprocation, consistency, social validation and scarcity are major human tendencies that can be exploited in social engineering attack themes (Sternberg, 2010). Barney (2015) argues that, unlike major corporate structures, caregivers within the medical community are naturally trusting individuals who are not steeped in strict technological expertise. This trusting human quality is exactly what Social Engineers need to ply their seemingly innocuous plans. Caregivers have a desire to be helpful and to look out for each other. This creates an opening for the Social Engineer. Finally, the persistent desire to avoid offending someone often supplants the tendency to exercise caution in dealing with others.

The clearest definition of Social Engineering within the Health Care field is that it is a means of gaining access to critical areas of security, privacy and clinical operations that bypass the very technologies and technical systems that are designed to protect it. Security is only as strong as its weakest link within the organization—people. The track record of Social Engineering engagements and compromises is aided and abetted by organizations that employ uneducated, untrained, careless or technologically naive caregivers (Malatesti, 2016). Social engineering in information security is the art of influencing the helpful employee to give up their sensitive information (Kaur and Singh, 2015). It describes a non-technical attack that relies on exploiting human interaction which facilitates bypassing normal security procedures.

There are two types of social engineering attacks (Kaur and Singh, 2015): human based social engineering (includes impersonation, being a third party, desktop support, shoulder surfing, dumpster diving etc.) and computer based social engineering (includes phishing, baiting, online scams, vishing, using social networking sites etc.). According to a recent study, healthcare data breaches on an overall basis cost the industry as much as $6 billion. There is an average organizational cost of $2.1 million for each breach, which involved incidents with an average of 2,700 lost or stolen records (Ponemon, 2015). Human error arising from carelessness on the part of staff, management or employees, as well as inadequate training, was the most important factor in this study. Additionally, organizations that fostered the concept of mandatory training of clinical staff at all levels and allowed them to understand how the slightest data security breach can lead to a major problem is the only way to tighten the security perimeter on the front line of healthcare.

One of the more interesting responses that arise in the realm of Social Engineering is the contention that it is more of a problem in Health Care than in other fields of human endeavor (Trinckes, 2015). Nurses, in particular, tend to be trusting. They have an innate desire to be helpful. They do not want to appear incompetent, especially in regard to technology. They do not want to offend others, particularly co-workers. They tend not to be whistle-blowers. All these are reasons that they may fall prey to social engineering techniques.

Behavioral issues in security governance suggests problems such as employee deviance, employee compliance, effective decision making and stressful conditions leading to higher risk in decision-making by staff (Zhou, et al, 2010). It is critical to understand such vulnerabilities in the organization and systematically address these in proactive security planning. Health Care organizations that utilize electronic and social media typically have policies governing employee use of such media in the workplace to prevent Social Engineering problems (Spector & Kappel (2012).

There is an increase in usage of mobile devices (laptops, smartphones, tablets) in the healthcare industry (Ventola, 2014), especially nurses and nurse practitioners. These devices are used to access, transmit, receive and store personal health information. The growth in usage of such devices can be attributed to their portability, relative use of ease and convenience (Storbrauck, 2015). The mobility helps practitioners to easily travel from patient to patient without being confined to their desk. Also, it is useful in completing health visits in patient's homes, clinic or other facilities and still have access to medical records. This convenience can lead to potential security threats and calls for enhanced and regular training to raise the awareness of healthcare providers (Storbrauck, 2015). Nurse practitioners have access to patient records on these devices and are allowed to use these devices at public places. This increases the risk for unauthorized access to information and loss or theft of device (Storbrauck, 2015). Theft of a mobile device is one of the most common causees (68%) of breach of personal health information (McCarthy, 2014). Healthcare service providers can misuse the mobile devices or access that have been provided to them on regular computer terminals as well. It is important to have strong encryption, as well as authentication protocols to make the devices less susceptible to unauthorized access. Having weak passwords or sharing of passwords can also create vulnerabilities that needs to be addressed (Storbrauck, 2015). Access control is mandated by HIPAA (HIPAA Security Series 2009). The intent is to prevent unauthorized access by anyone to the system and provide audit trails to detect the source of such access, in case a breach occurs.

In summary, health care workers are prone to social engineering attacks in their day to day work environment, especially in the area of access control privileges of employees, mobile device management and lack of training needed to understand the vulnerabilities factor. This study addresses these issues.

METHODOLOGY

Data Collection

A survey was conducted in healthcare informatics classes for undergraduates and graduate students. The survey consisted of 16 Likert Type questions focusing on three areas of social engineering; access to data, using mobile devices for patient record access, and training implementation. Three indices corresponding to each of the three areas were calculated.

A total of 91 subjects completed the survey (11% Male, 89% Female). Only 5.5% of the subject pool was older than 50, and 53% were between 20 and 29 years of age.. The rest of the subjects were evenly split among the two other age groups; 30-39 and 40-49 years old. The majority of students had a bachelor's degree (71.5%), with 5.5% having only an associates/trade school degree. Only 1 subject (1.1%) had earned a doctorate.

All members of the subject pool worked in a health care environment, with a majority of 48% categorizing themselves as floor nurses. Administrators made up 11% with the remaining members listed under "support" (11%) and "other" (30%) categories. Almost 56% of the subject pool came from larger organizations with over 50 employees with only 3.2% reporting having worked in organizations with less than 11 employees.

The level of computerization in their work environments was evenly split with 53% reporting working in a completely computerized environment, with the rest (47%) reporting working in a partially computerized environment. Over 45% of the subjects reported that they weren't aware of Social Engineering as a threat.

In all questions in the access section, the highest frequency result on every question was "strongly disagree". The questions were worded such that this would indicate a strong desire to limit access. Interestingly enough, the question in this group that had the lowest score concerned physicians and administrators overriding access permissions, suggesting this is an area for further investigation. It is unclear if this is a training issue, or an overt policy decision on the part of the heath care institution.

Similar to the previous section, the questions on using personal devices to access patient records all had the "strongly disagree" as the highest value, yet their mean values were lower than the access section.

The question "I am required to access health information only through approved devices and software in the organization" had the highest negative response with 66% selecting strongly disagree.

The questions on training had the largest spread of responses. In fact "agree" rather than strongly agree was the highest vale for the question, "I get adequate training in computer and security related things, to perform my duties effectively." This was the same for the efficacy of the training received as, "The training that I receive to perform my job effectively is relevant and helpful." This indicates that, while the subjects were still positive about their training environment, they felt less strongly about the training than they did about the importance of limiting access to patient records.

The most negative score in this section was the whistleblower question, "In my work place, whistle blower behavior is rewarded by the management." This question had an actual overall mean score in the above 3 (neutral) with 57% selecting that option.

Data Analysis

Two of the three indices, access and the use of mobile devices, were positively skewed, reflecting that the subject's response showed that limiting access to patient data is recognized as important in their work environments. This includes not using personal devices to access patient records.

There is a moderate Pearson correlation (.480) between the access and mobile device indices but no correlation between either of these and the training index. What is most surprising is the implication that there is no correlation between the subject's view of their training and their views on access to patient records, and the use of personal devices to access data. The data suggest that training is not the factor that leads to their views.

To look deeper into this result, ANOVA's were run using the index values and the individual demographic survey questions as factors. While most of the questions did not have a significant result, four did show significant differences between the groups.

Table 1. ANOVA Values Based on Groups

	ANOVA Significance level			
	Education level	Role	Length of Service	Size of Organization
Access	.003	.005	.005	.004
Mobile Devices	Not Sig	.046	.003	.013
Training	Not Sig	NS	Not Sig	NS

Education Level

This ANOVA did show a significant difference in the educational groups. Further analysis indicated that the group with a significantly different mean was the "High School" level group. In conjunction with the correlation data above, this indicates that limiting access to patient data is a trait that is developed during a bachelors' level education.

Role in Organization

Not surprisingly, given the results in educational level, the ANOVA for the role in the organization also showed a significant result. This time the "Support Role" was the factor that was significantly different from the others. This fits with the correlations and other ANOVA's to suggest that the lack of a bachelor's degree is the driving force behind these results and not work related training.

Length of Service

ANOVAs on the Length of Service questions had similar results to the role of the organization. The factor "Less than one year of Service" was the mean value that was significantly different from the rest in both the access index and mobile devices index. This would suggest that the organizational training and/or environment is a factor in the development of these traits as well as their access to a bachelor degree level of education.

Size of Organization

Small organizations, measured as those with 10 or fewer employees, had a significantly lower score on both the access and mobile indices. Unfortunately, the subject pool in small organizations was only three. This is too small a number of subjects to draw any meaningful insights from, but does suggest further areas for study.

DISCUUSSION

The results drawn in this study are interesting. Our data suggests that over 45% of the subjects reported that they weren't aware of Social Engineering as a threat. This is a disturbing trend. Employees in healthcare settings need to be aware of threats such as social engineering and need to get trained in case a situation arises causing vulnerability to the system and data. We also found that majority of subjects scored very high on their knowledge to keep patient records secure which is a good practice in creating an informal secure culture. Majority of subjects scored very high on their knowledge of not accessing patient records on mobile devices. This awareness is helpful in protecting patient information for getting exposed, stolen or compromised on a mobile device.

We also found that majority of subjects were happy with their level of current training on security related issues in their respective organizations. It is not clear whether this satisfaction comes from lack of knowledge about the real threat social engineering presents or the training is actually adequate to educate employees about such vulnerabilities. Our data suggests that whistleblower behavior is still less supported in organizations and it is not something that employees are comfortable with or are inclined to go that path.

Physicians and administrators are viewed as having different rules on access to patient records. This might be due the separation duty control built in the systems for provide right kind of access to employees based on their role. It also suggest that when it comes to violation of access rights in a given situation, physicians and administrators are viewed and treated differently that any floor staff such as a nurse or even an IT support personnel. Administrative support personnel scored lowest on the patient access and mobile use indices and subjects without a bachelor's degree scored lowest on the access index. It clearly suggests that people in administrative groups and ones without a bachelor's degree do not understand or enact the responsibilities of "right access" seriously. It is difficult to comment on the reasons of such attitude; it could be the administrative role that they perform makes them prone to overriding access or simply lack of education in this area.

Security is only as strong as its weakest link. Social engineers attack the weakest link in any business process—people. This makes it necessary to take the time and effort to mitigate Social Engineering incursions, which require a concentrated drive using policies and procedures that are formulated on an on-going basis through security awareness and training programs. Thus, security policies, training and awareness programs serve as the fundamental tools to promote a culture within the healthcare environment.

CONCLUSION

This study, in a healthcare setting, looks at the role of access of systems, usage of mobile devices and training provided to employees, in the context of social engineering attacks. The results suggested that there is a correlation between access permissions and mobile device usage. The implications of results are presented.

REFERENCES

Anderson, R. and Moore, T. (2008). Information Security Economics and Beyond, Information Security Summit, 2008

Barney, Brand. (2015) Heathcare: Recognize Social Engineering Techniques, Security Metrics.Com 2015, Retrieved from http://Blog.securitymetrics.com/2015/08/healthcare-social-engineering.html

Baym, N. K., Zhang, Y. B., & Lin, M.-C. (2004). Social interactions across media: Interpersonal communication on the internet,telephone and face-to-face. New Media & Society, 6, 299-318.

Gartner, A. (2015. The Rise of Multifaceted Social Engineering Attacks Paul Ekman Group. Retrieved from Https://Social-engineer.com/rise-social engineering attacks/gartner.html

Kumar, R. and Singh, H. (2015). A Framework to Mitigate the Social Engineering Threat to Information Security, *International Journal of Advance Foundation And Research In Science & Engineering (IJAFRSE), 1,* Special Issue , ICCICT 2015. Impact Factor: 1.036, Science Central Value: 26.54

Kaur, I. and Singh, G. (2015). Social Engineering technique to gather Critical Information of Social Networking Websites, *International Journal of Computer and Communication System Engineering (IJCCSE), 2*(4), 2015, 581-585.

Malatesti, Christian. (2016). Social Engineering Attacks. Enterprise Risk Management. Retrieved from http://www.emrisk.com/knowledge-center/white-papers/social -engineering-attacks.html

McCarthy, K. (2014). Study: Majority of healthcare data breaches due to theft. Retrieved March 27, 2015.

Palmgreen, P., Wenner, L. A., & Rayburn, J. D. (1980). Relations between Gratifications Sought and Obtained: A Study. *Communication Research, 7*, 161-192

Mishra, S. (2015). *Organizational Objectives for Information Security Governance: A Value Focused Assessment,* Information Management & Computer Security.

Sternberg, G. (2010). The Psychology Behind Security. *ISSA Journal.* Retrievedfrom http://www.issa.org/images/upload/files/SternbergPsychology%20Behind%20Security

Storbrauck, Lauren, "Mobile Device Use: Increasing Privacy and Security Awareness for Nurse Practitioners" (2015). *Economic Crime Forensics Capstones.* Paper 7

Spector N. and Kappel, D. (2012) ”Guidelines for using Social Media”. The Online Journal of Issues in Nursing”, Volume 17, Number 3.

Trinckes, J. (2016).The Surprising Weakest Link in the Information Security Chain. Retrieved from http://www.hitechanswers.net/informaion-security-social engineering.html./

The HIPAA Privacy Rule and electronic health information exchange in a networked environment: accountability (2009).

Ventola, C. (2014). Mobile Devices and Apps for Health Care Professionals: Uses and Benefits. *Pharmacy and Therapeutics, 39*(5), 356-364. Retrieved from http://www.ncbi.nlm.nih.gov/pmc/articles/PMC4029126

Whiteside, T. (1977) “Dead Souls in the Computer”, The New Yorker, August 27, 1977, Page 35.

Zhou, C. V., Leckie, C., & Karunasekera, S. (2010). A survey of coordinated attacks and collaborative intrusion detection. *Computers and Security, 29*(1), 124–140.