MWAIS 2015 Proceedings

Midwest (MWAIS)

Spring 5-14-2015

A prototype for continuous security awareness in financial institutions

Arnold Nzailu
Dakota State University, abnzailu@pluto.dsu.edu

Raj Kumar Nepali
Dakota State University, rknepali@pluto.dsu.edu

A prototype for continuous security awareness in financial institutions

Arnold Nzailu
Dakota State University
abnzailu@pluto.dsu.edu

Raj Kumar Nepali
Dakota State University
rknepali@pluto.dsu.edu

ABSTRACT

Information security is recognized as a management issue. Sarbanes-Oxley specifies that management is ultimately responsible for the security, accuracy, and privacy of information relating to corporate financial records and by ricochet the protection of Personally Identifiable Information (PII). Many organizations have established information security program. One of the key components of an information security program is to build security awareness as humans are considered as the weakest link of the security chain. In order for security awareness programs to add value to an organization and stay effective against the threat against human hacking, it is important to measure and continuously improve its effectiveness. This paper uses design science research approach to propose a prototype for continuous security awareness improvement in financial institutions. The prototype will be contribution in the information security field and will guide decision makers at financial institutions in their choice of security awareness product.

Keywords

Prototype, security awareness, continuous security.

INTRODUCTION

A multitude of risks threatens the operations of organizations, which nowadays is often grounded on insecure application of information technology and information systems (Bauer & Frysak, 2014). The year 2013 may be remembered as the "year of the retailer breach" but a comprehensive assessment suggests it was a year of transition from geopolitical attacks to large-scale attacks on payment card systems (Verizon, 2014). The importance of information security cannot be overemphasized in today's networked world. Previous research identified humans as major enablers for loss events, especially if humans use information technology to carry out their work. Kevin Mitnick, arguably one the world's most famous hacker, testified to the US Senate committee that he had obtained more passwords by tricking users than by cracking (Goh, 2003).The human side of computer security is easily exploited and constantly overlooked. Companies spend millions of dollars on firewalls, encryption, and secure access devices; however it does not help to improve security posture if the organizations lack security culture. Many consider it as money wasted, because none of these measures address the weakest link in the security chain, the humans (Sasse, Brostoff, & Weirich, 2001). A major component of reducing the risk of security breach in information asset is by implementing an effective security awareness program in organizations (Martinez, Turabo, & Cleal, 2010)

Although there is a large number of research in the area of security awareness (Kritzinger & Smith, 2008; Tsohou, Karyda, Kokolakis, & Kiountouzis, 2012; Valentine & Labs, 2006), there has been little or no research literature about continuous security awareness programs in the financial sector. Most security awareness programs are comparable to IS audit in that they are point in time activities. IT security can only improve if it can be measured. However, defining metrics to measure information security is tough and sometimes undoable process. Since security awareness is part of information security, it is reasonable to argue that the same holds for security awareness (Spruit & Roeling, 2014).The purpose of this paper is to build a prototype for continuous security awareness programs for information protection in financial institution. The prototype will be use as vital complements to other defensive tools in the security officer toolbox.

THEORETICAL BACKGROUND

Through the years, a number of theoretical perspectives have been applied to provide an understanding of information technology adoption and use; including behaviorist theory of learning, theory of reasoned action (TRA), theory of planned behavior (TPB), and technology acceptance model (TAM). The design and the development of the artifact in this research effort will be greatly influenced by these well-known theories that have been successfully used in pass literature (Al-Omari, El-Gayar, & Deokar, 2012; Bulgurcu, Cavusoglu, & Benbasat, 2009; Gong, Xu, & Yu, 2004).

Technology Acceptance Model

The technology Acceptance Model (TAM) developed by Davis (1989) has emerged as one of the widely used model in the study of information system adoption . The TAM has adapted the TRA and hypothesized that a person's acceptance of a technology is determined by his or her voluntary intention to use that technology. Additionally, it has hypothesized that Intention is determined by the person's attitude toward the use of that technology and his or her perception concerning its usefulness. In TAM, Attitudes are formed from the beliefs a person has about the use of the technology. Two particular believes are expressed in the model. The first belief, perceived usefulness (PU), is the user's "subjective probability that using a specific application system will increase his or her job performance" The second belief, perceived ease of use(PEU), is "the degree to which the user expects the target system to be free of efforts" (Davis, 1989). Figure 3 illustrates the relationship between the different construct of the TAM.

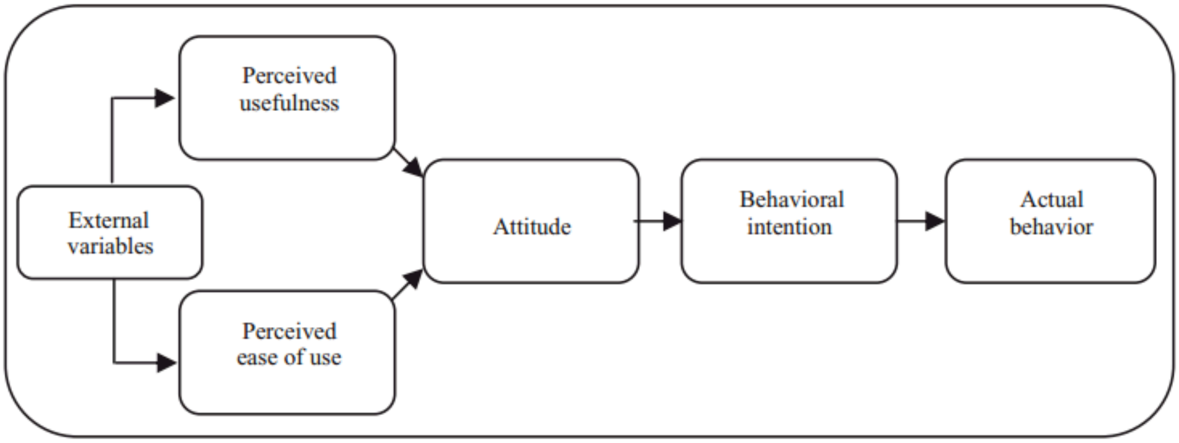

Figure 1. Technology Acceptance Model (Davis, 1989)

Although all three theoretical models (TAM, TRA, and TPB) are relevant in our research effort, the design of the artifact will base on the technology acceptance model (TAM). TAM will be the focus because of three factors: (a) it is prudent, IT-specific, and designed to provide an adequate explanation and prediction of a diverse user population's acceptance of a wide range of systems and technologies within varying organizational and cultural contexts and expertise levels; (b) it has a strong theoretical base and a well researched and validated inventory of psychometric measurement scales, making its use operationally appealing; and (c) it has accumulated strong empirical support for its overall explanatory power (Mathieson, 1991; Szajna, 1996)

RESEARCH METHOD

Building an information security artifact requires a structured approach. Since our goal is to build a prototype, It will be suitable to use the design science research method share by Hevner et al. (2004). Hevner et al. (2004) point out the consecutive steps to be followed and explicitly state requirements for any study to be qualified as design science research. Design Science research heavily relies on the body of knowledge of the particular research domain. The bases for our investigation and proposed prototype are emerging from the literature on security awareness, learning theories, behaviors modification theories and quality improvement principals. The figure below shows an overview of the project plan.

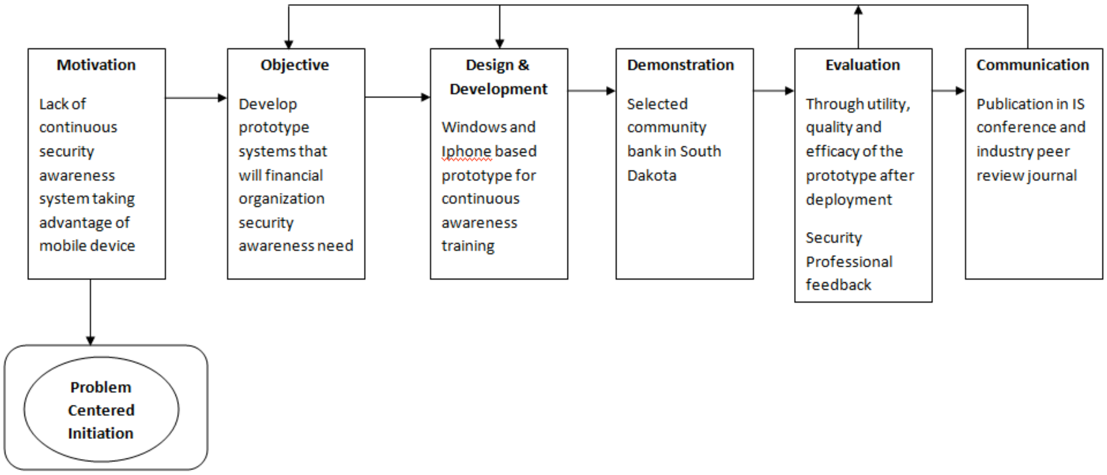
Motivation
Lack of continuous security awareness system taking advantage of mobile device
Objective
Develop prototype systems that will financial organization security awareness need
Design & Development
Windows and Iphone based prototype for continuous awareness training
Demonstration
Selected community bank in South Dakota
Evaluation
Through utility, quality and efficacy of the prototype after deployment
Security Professional feedback
Communication
Publication in IS conference and industry peer review journal
Problem Centered Initiation

Figure 2. Project Plan

DESIGN AND DEVELOPMENT

In this research, we propose a four stages design process. On stage one, we will develop Security Awareness knowledge repository; a database of security questions and knowledge material based on generic roles that exists in financial institution such as teller, loan officer, customer service, president, system administrator, and others. Each security question will have attribute expressing the difficulty level. An additional requirement of this stage is that the Security Awareness knowledge repository must be easy to update.

Stage two will focus on the Security Awareness decision engine and Security Awareness Assessment Result Database. The decision engine will be integrated with an active directory or LDAP (Lightweight Directory Access Protocol) to allow the decision engine to retrieve user role on user login. In addition to user roles retrieved from active directory, the decision engine will make use of a measurement framework such as the Item Response Theory (IRT). The Item Response Theory has been extensively used in the design and analysis of educational and psychological assessments such as the ACT, GRE, GMAT and other standardized tests (Wikipedia, n.d.). Results from security questions will be stored in Security Awareness Assessment Result Database. This database stores results from both the initial security awareness assessment and the ongoing security awareness assessment. Additionally, this database will also keep track of the daily security tips sent to the users by the decision engine.

Stage three will be dedicated to the user interface design. User interface includes IPhone application that will receive the notifications containing security awareness knowledge every morning between the hours of 6AM and 9AM. The knowledge received will be related to security question that the user will have to answer to finish the desktop login. The desktop user interface will be a web-based interface locking the screen and presenting the user a security awareness question at each login. This process will mimic the process used by public library to inform the patrons of the computer acceptable user policy.

The fourth and the last stage of the design will be the development of reporting capability for the prototype. Report will be generated using the results obtained from correctly answered or incorrectly answered questions. The reporting capability will allow trend analysis of users' security awareness in general and user personal security awareness level. The report will give management a point in time view of the overall security awareness posture of the organization as a whole as well as business unit.

The assumption is that a Security Awareness Assessment test will be required for all employees. The security awareness assessment test will be used to establish the baseline to measure the security knowledge of new employee and internal transfers. Two types of security assessment questions will be programmed for each employee. The first type will consist of general security questions, while the second type will be based on the employee role. The results of both assessments are sent to the Security Awareness Assessment Result database, which will then be used by the decision engine. Figure 3 below shows the overall functionalities of the proposed prototype.

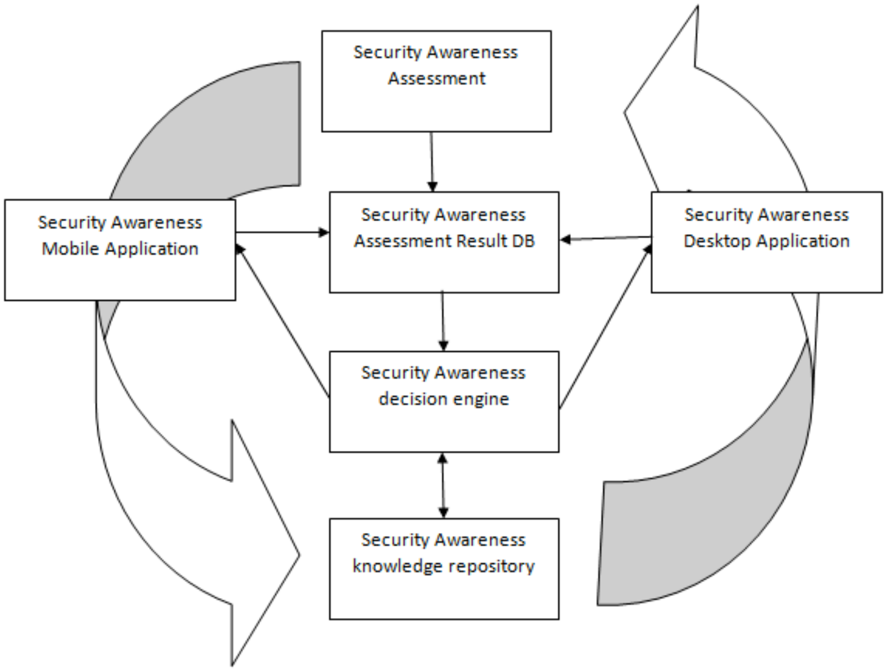
Security Awareness Assessment
Security Awareness Mobile Application
Security Awareness Assessment Result DB
Security Awareness Desktop Application
Security Awareness decision engine
Security Awareness knowledge repository

Figure 3. Prototype Functionalities

ALGORITHM

```
Input: Get the role of employee from AD

1 begin

2  If  new employee or internal transfer then:

         Security Awareness Assessment

3 else:

       i. Send Security Knowledge to smart phone
       ii. Send assessment question from decision engine to desktop
       iii. Receive the answer from employee and send the result to the Assessment Result database
       iv. Decision engine compares result with the baseline for employee role

       v. if grade above baseline for position then:
                    increase complexity for user
          else:
                    decrease the complexity
                    send users link to reading material

4 end
```

EVALUATION AND VALIDITY

The evaluation part of the research effort is one of the most important parts of the entire project. In Design Science Research, we are concerned with the evaluation of design science outputs, which may include theory and/or artifact. For this research, a single case study with a holistic view will be performed because the prototype will be evaluated for the whole organization and no distinction will be made between various departments. Hevner et al. (2004) identify evaluation as "crucial" and require researchers to demonstrate the utility, quality, and efficacy of a design artifact using rigorous evaluation methods. Therefore, the evaluation of the artifact will be performed using the above-cited criteria. Quality and efficacy of a design artifact will be demonstrated by the functional and structural testing. Utility will be evaluated by interviewing industry professionals and users of the system.

Validity is another important aspect of research. The formative and summative validity will be achieved by following the prescription from Lee & Baskerville (2003). Formative validity will be achieved by following accepted procedures to design the artifact. The artifact design will be based on the literature review and a periodic discussion with information security professional. Summative Validity will be achieved by ensuring that the Artifact does what it is supposed to do: increasing security awareness.

CONCLUSION & FUTURE WORK

The prototype is intended to make employees more aware of potential information security risks and reduce the risk of human hacking. Compared to conventional methods, the prototype will add to the knowledge base, a method to deliver continuous information security awareness in an effective and efficient way. Further research will look into comparing security awareness level of an organization using the proposed prototype and one not using the prototype. Additional research could be performed using The Theory of reasoned action (TRA) or The Theory of Planned Behavior (TPB) to deepen the understanding of the adoption or the rejection of such a system like the one proposed in this paper.

REFERENCES

Al-Omari, A., El-Gayar, O., & Deokar, A. (2012). Security Policy Compliance: User Acceptance Perspective. In *2012 45th Hawaii International Conference on System Sciences* (pp. 3317–3326). IEEE. doi:10.1109/HICSS.2012.516

Bauer, S., & Frysak, J. (2014). Developing a Viral Artifact to Improve Employees ' Security Behavior, (8), 2420–2423.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2009). Roles of Information Security Awareness and perceived fairbess in Information Security Policy, *2009*, 1–11.

Davis, F. D. (1989). Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology. *MIS Quarterly*, *13*(3), 319–340. Retrieved from http://www.ezproxy.dsu.edu:2048/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=keh&AN=4679168&site=ehost-live&scope=site

Goh, R. (2003). Importance of the Human Element Dissertation.

Gong, M., Xu, Y., & Yu, Y. (2004). An Enhanced Technology Acceptance Model for Web-Based Learning. *Journal of Information Systems Education*, *15*(4), 365–374. Retrieved from http://www.ezproxy.dsu.edu:2048/login?url=http://search.proquest.com/docview/200114529?accountid=27073

Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design science in information systems research. *MIS Quarterly*, *28*(1), 75–105.

Kritzinger, E., & Smith, E. (2008). Information security management: An information security retrieval and awareness model for industry. *Computers & Security*, *27*(5-6), 224–231. doi:10.1016/j.cose.2008.05.006

Lee, A. S., & Baskerville, R. L. (2003). Generalizing Generalizability in Information Systems Research. *Information Systems Research*, *14*(3), 221–243. doi:10.1287/isre.14.3.221.16560

Martinez, E. M., Turabo, U., & Cleal, M. G. (2010). A framework for information security awareness programs, *XI*(1).

Mathieson, K. (1991). Predicting User Intentions: Comparing the Technology Acceptance Model with the Theory of Planned Behavior. *Information Systems Research*, *2*(3), 173–191. Retrieved from http://www.ezproxy.dsu.edu:2048/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=keh&AN=4431053&site=ehost-live&scope=site

Sasse, M. A., Brostoff, S., & Weirich, D. (2001). Transforming the "weakest link" — a human/computer interaction approach to usable and effective security. *BTexact Technologies*.

Spruit, M. R., & Roeling, M. (2014). ISFAM: the Information Security Focus Area Maturity model ISFAM: *Proceedings of the Twenty Second European Conference on Information Systems, ECIS 2014*.

Szajna, B. (1996). Empirical Evaluation of the Revised Technology Acceptance Model. *Management Science*, *42*(1), 85–92. Retrieved from http://www.ezproxy.dsu.edu:2048/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=keh&AN=9606262589&site=ehost-live&scope=site

Tsohou, A., Karyda, M., Kokolakis, S., & Kiountouzis, E. (2012). Analyzing trajectories of information security awareness. *Information Technology & People*, *25*(3), 327–352. doi:10.1108/09593841211254358

Valentine, J. A., & Labs, I. (2006). Enhancing the employee security awareness model, (June), 17–19.

Verizon. (2014). *2014 Verison data breach report*.

Wikipedia. (n.d.). Item Response Theory.