SECURITY AWARENESS AND TRAINING IN THE SOCIAL COMPUTING ERA: MODELING BEHAVIORAL CHANGE IN A HYPER-CONNECTED ENVIRONMENT

Anne-Marie Guidy-Oulai and Alan Rea
Department of Business Information Systems, Haworth College of Business
Western Michigan University, Kalamazoo, MI 49008-5412, USA

ABSTRACT

In recent years, the influx of social computing represented by Facebook, Twitter, and a myriad of social sites presents a unique security challenge to organizations. Blocking a website on the enterprise network is only a bandage on the much larger challenge of information protection when leakage occurs via a wide array of avenues to include smart phones, tablets, and other mobile devices. In this paper, we provide an overview of the organizational challenges within this hyper-connected environment and propose a revised model for security education that takes into account the massive influx of social computing within organizational contexts.

INTRODUCTION

Computing systems have become the de facto tools for collecting and processing data, as well as providing massive amounts of information.   In the organizational sector this has been the case for many years and security professionals have developed tools and approaches to ensure the confidentiality, integrity, and availability of these systems and the data they contain.

SECURITY POLICY EVOLUTION

However, the security professional’s toolkit has changed dramatically over time. This is best illustrated in the evolution of how we have approached secure systems via system and security policies (White & Rea, 2008). First-generation system policies primarily focused on checklists for specific solutions that focus on "what can be done rather than what needs to be done" (Baskerville, 1993, p. 381). Although we might be quick to argue these are no longer used, one only needs to go as far as help desk checklists designed to address general computing problems, or user manuals for a variety of peripheral devices. First-generation policies are easy for users to follow as long as there are no outliers that would cause the steps or checklist to fail. In the security realm we still see attempts to implement these policies in areas such as wireless home router setup steps and checklists (Chen et al, 2006; Kritzinger and Smith, 2008).

Anyone running into challenges with a home network setup can envision how this increases in magnitude within an organization setting. Connecting a printer via a USB cable is inherently simpler than networking a printer and sharing it among home users. In the contemporary connected realm of computing we tend to see more interaction and a need for connected systems.

The richness of a connected system adds to its complexity. It is this complexity that brings us to second-generation system policies. Here, we move from checklists and steps at the physical level to more conceptual security concepts. Many highly-technical system procedures in use today are based on second-generation security policies. It is here we also see the emergence of system requirement specifications such as entity relationship diagrams to determine system and security needs.

This interconnectedness does not automatically imply social connectivity (even if a printer is shared). To underscore this Baskerville notes that second-generation approaches focus on the mechanistic aspects of systems (Baskerville, 1993, p. 400) rather than business process needs that can result in functionality versus security conflicts (Baskerville, 1993, p. 401). We are all well aware that when users are not part of the system design process that implements a secure mechanism, there is a tendency for users to find a "work-around" in order to efficiently complete their tasks. Many times these lead to lapses in security procedures (e.g., computer passwords taped to monitors).

Of course, we know now that systems designed for security without considering human interaction will be compromised. It is this shift into taking the social into account that moves us into third-generation model to include both behaviors and organizational needs (Baskerville, 1993, p. 402). In the early nineties there were not many third-generational systems to analyze, but Baskerville's (Baskerville, 1993) work has been built upon and expanded with the influx of organizational system integrations.

One such expansion discusses how Baskerville's (Baskerville, 1993) third-generational model does not quite take into the account what we now consider social although it does address organizational conditions within this context (Siponen, 2001). Siponen (2001) creates a fourth-generational socio-technical approach where the communication between responsible system parties is "understandable for both normal users and system designers – therefore breaking the possible communication gap" (Siponen, 2001, p. 115). In this approach we can see the true complexity and interconnected system matrices inherent in organizational systems. In order to create effective security training and awareness programs we must address how system, processes, and people are intertwined.

SOCIAL COMPUTING VERSUS SOCIAL NETWORKING

The intertwined nature comes to the forefront when we examine current organizational computing contexts. The explosion of social computing has changed the way many people work with computer systems and mobile devices. People share photos with thousands at the click of a button (e.g., Instagram) or check social news aggregators (e.g., newsvine) rather than their local news site. The strengthened sense of an extended community offered via social networking offerings such as Facebook and Twitter often blurs the lines between work and social spheres more so than ever before.

Both social computing and social networking are vibrant approaches to sharing information and creating collaborative content. In current research there is little distinction between these terms. Most researchers describe social computing with large brush strokes (Pascu et al, 2008; Wang et al, 2007).   This is an acceptable approach because it includes connected applications that "share high degree of community formation, user level content creation, and computing" (Parameswaran & Whinston, 2007). In other words, social computing is identified by information sharing to facilitate collaborative content creation. Social interest communities form around various topics whether they are news, research, or entertainment oriented.

Social networking is a subset of social computing rather than an entirely different entity. In social networking studies researchers look to the specific communication avenues between entities (e.g., business and customer) that lead to satisfaction or a sense of loyalty (Cho, 2008) or how the various interactions among users can build strong support networks (Chung, 2001). In this sense, social networking focuses less on collaborative content building and more on information sharing and relationships.

We make the distinction between the two approaches because organizations need to address them differently when and help employees understand the implications for use (and misuse) in policies. For example, it might be perfectly acceptable for an accountant to donate her personal time to a non-profit area of a social computing site creating frequently-asked question pages or participating in Web discussion boards as long as she does not identify herself as an employee of the company. However, this same accountant might cause issues if she shared personal observations on how to improve company accounting process via her Twitter account instead of using established organizational communication channels even if her Twitter followers are the same people from the non-profit social computing site.

Ultimately both social computing and social networking promote collaboration and information sharing. These concepts are many times in conflict with information security policies and procedures. However, rather than being seen as an anathema to secure computing that must be excommunicated, social computing and social networking must be addressed via security awareness and training. Employers need to make their expectations known; employees must be aware and understand the accepted policies and procedures for using their technologies.
The most effective means to communicating this awareness and understanding it is through social security education.

SOCIAL SECURITY EDUCATION

In the past, information security professionals could minimize lost productivity by simply blocking select websites via the firewall (Cho, 2008). If company policy was in place that limited users from visiting social networking sites or other distractions an organization could effectively stop employee use of these offerings on workplace systems. Of course, the line blurs for those with laptops who are expected to use them outside of the office. Company policy needs to be clear as to whether these systems can also be used for personal endeavors (e.g.,Facebook).

However, it is the influx of tablets (e.g., iPad) and smartphones that is truly blurring the work/personal distinction. Many employees are demanding that they be permitted to use these devices to help them do their work. Some companies purchase and control the devices, but many simply provide an allotment or allow personal devices within the corporate network. Although it is challenging enough to create robust access policies and controls to protect organizational information from leakage, it is even more challenging to educate employees on the appropriate usage of social networking within the work/home environment as it relates to overall corporate image and impact.

Current security education and policies are just beginning to grapple with how to control the hybridization of computing. In its truest socio-technical form, employees bring smartphones to work that access both corporate and personal information. One would hope that an employee would know better than to complain about a manager or task on Twitter, but the high-speed 140-character info blurb has become the norm and does not always lend itself to thoughtful reflection and processes. If those in the workplace follow an employee and re-tweet, the word spreads. If the employee has linked to Facebook or LinkedIn, the damage may multiply as connections enable others (to include competitors) to learn about personnel issues within an organization.

PAPER ORGANIZATION

Given the growing influx and usage of social networking within the organization and personal context, we must re-examine existing security education models and approaches within this hyper-connected environment. Using a socio-technical approach, our model builds on others discussed in the following section. Although our model centers on measuring behavioral change as an indicator of success (Hassel and Wiedenbeck, 2004; Wolf, 2011), it includes strong awareness of the various permeations between work and personal space that cannot be found in most current security training and awareness techniques and approaches.

The remainder of our paper is as follows. In the next section we examine current security education approaches to understand what they cover, as well as where there is room for improvement. We then put forth our model that takes into account not only the socio-technical approach but also the trend in social information leakage via social networks. Following the model discussion, we present our current study and evaluation instrument. Finally, we suggest how organizations might improve their security awareness and training given the current hyper-connected environment.

LITERATURE REVIEW

The ultimate goal of information security is to protect information from intentional or accidental misuse inside or outside the organization; it must also support and protect the three pillars of information security: information integrity, availability, and confidentiality (Johnson, 2006; Kritzinger & Smith, 2008). However, these three pillars not only continue to be a challenge in traditional security environment but also are exponentially increased in socially-infused organizations.

Security Awareness Challenges

Current organizations are constantly reacting to and addressing critical security incidents no matter how prepared they may be (Eminagaoglu, 2010; Rhee et al, 2012). This is primarily due to the increased dependency on networks in business environment during the last decade and the recent emergence of social computing (Shaw et al, 2009). Securities technologies such as anti-virus software, firewalls, Virtual Private Networks (VPN), and anti-spyware software are implemented by companies (CSI, 2010) on a regular basis, many times following accepted information security standards. However, technology alone cannot solve problems associated with information security threats. Regardless of the type of security technology used by organizations, information security will not be effective if users do not understand its importance, their individual security responsibilities, and how to handle information in a secure manner. Therefore information security awareness has received a great deal of attention by information technology (IT) professionals as a means to increase organizational security.

Security awareness is critical for information security program and is many times seen as the weakest link in the "security chain." The main objective of information security awareness is to make users understand the numerous computer security risks and the importance of practicing safe computing behavior (Aytes & Connolly, 2004). Users' awareness is the main contributor to information security success and is less costly than more advanced technical implementations that are not as effective. If users are aware of security issues, they change their behavior and are able to better protect themselves as well as organizational data (Ernest & Young, 2004; Johnson, 2006; May, 2008; Wolf, 2011). Most security breaches are associated with human error (i.e., social engineering depends on it) not with the security technology itself. Statistics show that information security breaches from inside organizations both unintentional and intentional is much higher than other attack vectors. According to ISACA (2005), about 30-50 % of information security breaches are from internal sources. The CSI survey conducted in 2009 reported that an overwhelming majority of the computer security breaches are from inside the organization. It is the responsibility of organizations to make sure that their information security awareness procedures and policies are implemented to address human error and insider threats.

However, even though many companies provide security awareness, the standard used varies from organization to organization. Among companies that provide security awareness, not many measure their training effectiveness. The literature provides little information on how to measure the effectiveness of these programs and it becomes more complicated when social computing enters the picture.

Social Computing Influx

One of the growing areas of information technology today is social computing. Social computing differs from traditional organizational computing and content sharing in that it empowers organizations to conduct a dialog with both current and potential customers as well as increase their content distribution and marketing goals to a large segment of computer users who are already presently using the very same content medium (e.g., Facebook) However, social computing is a double-edged sword in that businesses not only must create useful content but also respond to various customer requests for dialog, criticism, etc. or risk losing followers or market share.

Businesses can work to create viable market plans and strategies to deal with content and external user interactions. Moreover, new Internet marketing strategies are part of most contemporary business plans. However, this is not the focus of our research. Instead we look at what business should do to education its employees on the correct use of social computing not only when using it in a professional manner but also when using social computing within each employee's individual dealings that might impact the organization. This becomes important because social computing empowers individual users sometimes with little technical abilities, and promotes decentralization, yet at the same time does not provide concrete demarcation points between personal and organizational usage. Businesses that fail to provide employees guidelines will, sooner or later, fall into one of the newer CSI attack vectors of instant messaging abuse (2007), intellectual property loss via mobile devices (2008), or exploits of user's social network profiles (2009). Unfortunately, the literature provides little information on security awareness programs specific to social computing. We aim to remedy this situation via our research.

Social Computing Awareness Training

The major challenge that organizations encounter is finding an appropriate method of information security awareness training for employees that will trigger behavior change. Most companies fail to provide an effective awareness program that will address management needs as well as technical and non-technical staff. Employees are not always aware of their individual responsibilities and accountability when it comes to information security. Add social computing to the mix and the challenge greatly increases. We propose that continuously measuring employee's awareness of information security will help the organization solve most of the problem associated with security breaches. However, employees must first be trained to be aware. Security is a significant issue in social computing today because content-delivery and collaboration platforms are highly decentralized, poorly governed and easy to access (Parameswaran &Whinston, 2007). This combination increases the risk of malicious, as well as unintentional activities due to rapid content dissemination (e.g., Twitter).

THE SOCIAL COMPUTING SECURITY AWARENESS TRAINING MODEL (SCSAM)

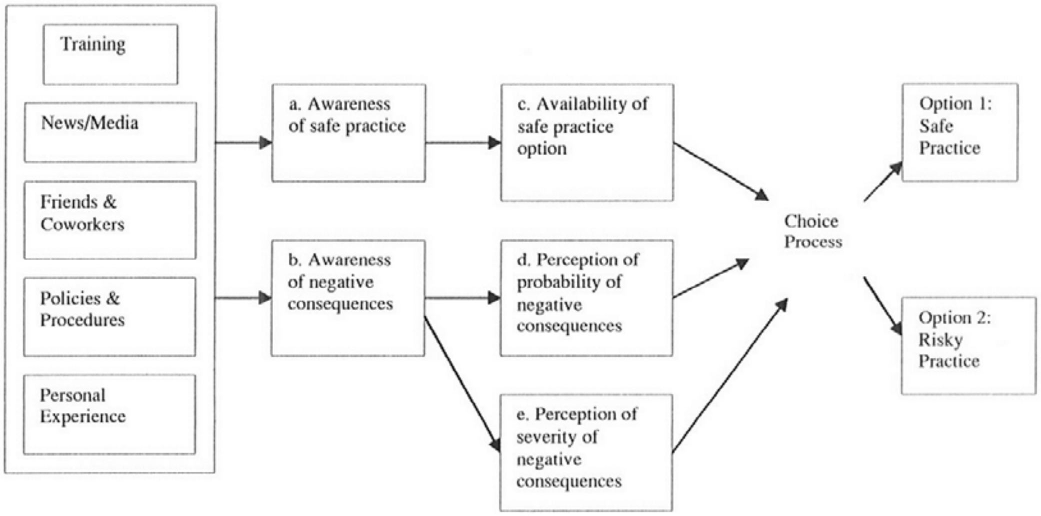
Our proposed Social Computing Security Awareness Training Model (SCSAM) builds upon the Rational Choice Model (Figure 1) developed by Aytes and Connolly (2004). The Rational Choice Model underscores the belief that people are somewhat guided by informed rational choices and will practice safe computing behaviors if they are aware of what this entails. Their model is founded on two theories: 1)Fishbein & Ajzen's (1975) Theory of Reasoned Act (TRA), and 2)Davis, Borgozzi & Warshaw's (1989) Technology Acceptance Model (TAM). Both theories are widely accepted in the information systems discipline and they argue that the use or non-use of information systems is a direct result of behavioral intentions.   The Rational Choice model extends the assumption that behavioral intentions are based on a user's rational choice that users make. Moreover, this choice depends on a user's perception of the standard behavior. Therefore, if users are aware of safe practices as well as negative consequences, their rational understanding and process will impact their choice.

Selection Rational Choice Model

Even though the Rational Model has been cited in numerous publications, it has not been extended in other research. Most criticized the model by arguing that people are not generally governed by reason, and the social environment is comprised of non-rational elements (Hassel & Wiedenbeck, 2004). Most suggest that any model involving human interaction must include non-rational elements. In this critical aspect we agree.

However, despite the criticisms of the Rational Model, a number of elements make it invaluable to training awareness. One of the main arguments for adopting this model as a major SCSAM influence is that it not only includes training but also awareness of safe practices, as well as negative consequences of unsafe practices. Since human factors are cited as the primary reason for computer security breaches, we must look at how people make choices. The Rational Choice model is used as a starting point because it has a firm basis in choice. However, the SCSAM adds three critical measurement criteria to the mix: 1) social computing elements that place proprietary and confidential information at risk, 2) guidance on social networking outside of company time and property, and 3) increased risk of online scam resulting in data or identity theft. In addition to social computing elements, the SCSAM incorporates measurement methods because a viable and robust security awareness program must measure success.

Figure 1: Rational Choice Model


Training
News/Media
Friends & Coworkers
Policies & Procedures
Personal Experience
a. Awareness of safe practice
b. Awareness of negative consequences
c. Availability of safe practice option
d. Perception of probability of negative consequences
e. Perception of severity of negative consequences
Choice Process
Option 1: Safe Practice
Option 2: Risky Practice

(Source: Aytes & Connolly, 2004)

PROPOSED SCSAM IMPLEMENTATION

We are currently formulating the complete SCSAM model. Once it is completed, it will be tested using companies with a strong social computing presence. Since social computing is a new way of conducting business, its security requirements may be drastically different from the traditional security awareness. We will measure this difference in our model as we look to create a viable SCSAM to address specific to social computing security needs.

Once the SCSAM is in place, we will measure its effectiveness through a series of qualitative interviews with participants from selected organizations. These participants will include upper-level management, as well as technical and non-technical personnel. We will interview information security practitioners as well. After the interview process, we will create an instrument based on our revised model and deploy it to the same organization. From there, we will analyze the results and present our findings.

CONCLUSION

Social computing and social networking have become prevalent forms of technology used by many organizations today. While these technologies may allow organizations to improve communication and productivity, security remains a main concern. Since social computing platforms encourage people to share personal information, employees may not be aware of how their actions online may compromise their company's security or reputation. Even the most careful and well-meaning employees can unintentionally post information they should not on company-approved social networking platform. Educating employees on company policies and social computing security awareness is a requirement for any contemporary organization. While privacy is well researched in the literature, and an array of security training awareness programs has been proposed, there are not many training programs that incorporate social computing. In our paper we have reviewed how social computing has evolved, and proposed a model for security training awareness that will incorporate the elements specific to social computing such as proprietary and confidential information leakage using social networking outside of company time, and awareness of social engineering via user profiles resulting in data or identity theft.

REFERENCES

[1] Aytes, K. and Connolly, T. (2004). "Computer security and risky computing practices: A rational choice perspective", *Journal of Organizational and End User Computing*, 16(3), 22-40.

[2] Baskerville, R. (1993). "Information Systems Security Design Methods: Implications for Information Systems Development", *ACM Computing Surveys (CSUR)*, 25 (4), 375-414.

[3] Chen, C. et al. (2006). "Mitigating Information Security Risks by Increasing User Security

Awareness: A Case Study of an Information Security Awareness System", *Information Technology, Learning, and Performance Journal*, 4(1), 1-14.

[4] Cho, Y., (2008). "Effects of Social Networking Sites (SNSs) on Hyper Media Computer Mediated Environments (HCMEs)", *International Business and Economic Research Journal* 7(7), 27-40.

[5] Chung, J. (2011). "Benefits of social networking in online social support groups", Humanities and Social Science, 71(9-A).

[6] CSI (2009). "The 14th Annual Computer Crime and Security Survey", *Computer Security Institute.*

[7] CSI (2010). "The 15th Annual Computer Crime and Security Survey", *Computer Security Institute.*

[8] Davis, F., et al. (1989). "User Acceptance of Computer Technology: A Comparison of Two Theoretical Models", *Management Science, 35(8), 982-1003.*

[9] Eminagaoglu, M., et al (2010). "The positive Outcomes of Information Security Awareness Training in companies- A Case Study", *Information Security technical Report*, 14, 223-229.

[10] Ernst & Young (2004). "Global Information Security Survey", retrieved from http://www.issa-motorcity.org/files/GlobalInformationSecuritySurvey2004.pdf , March 19, 2012

[11] Fishbein, M., & Ajzen, I. (1975). "Belief, Attitude, Intention, and Behavior: An Introduction to Theory and Research". Reading, MA: Addison-Wesley.

[12] [Hassel, L., & Wiedenbeck, S. (2004). "Human Factors and Information Security", retrieved from http://repository.binus.ac.id/content/A0334/A033461622.pdf, March 29, 2012.

[13] Johnson, C. (2006). "Security Awareness: Switch to a Better Programme", *Network Security*, 2006(2), 15-18.

[14] Kritzinger, E., and Smith, E. (2008). "Information Security Management: An Information Security Retrieval and Awareness Model for Industry", *Computer & Security*, 27, 224-231.

[15] May, C., (2008). "Approaches to User Education", *Network Security*, September 2008, 15-17.

[16] Parameswaran, M., and Whinston, A.B. (2007). "Social Computing: An Overview", *Communications of the Association for Information Systems 19*(37), 762-780.

[17] Parameswaran, M., and Whinston, A.B. (2007). "Research Issues in Social Computing *", Journal of the Association for Information Systems, 8(6), 336-350.

[18] Pascu, c. et al.(2008). “Social computing: implications for the EU Innovation Landscape”, The Journal of Futures Studies, Strategic Thinking and Policy, 10(1), 37-52.

[19] Rhee, H-S, et al. (2012). “Unrealistic Optimism on Information Security Management”, *Computer and Security* DOI:10.1016/j.cose.2011.12.001.

[20] Shaw, R.S., et al (2009). “The Impact of Information Richness on Information Security Awareness Training effectiveness”, *Computers & Education* 52, 92-100.

[21] Siponen, M. (2001), “An Analysis of the Recent IS Security Development Approaches: Descriptive and Prescriptive Implications”, in *Information Security Management: Global Challenges in the New Millennium*, eds. G. Dhillon, Hershey: Idea Group.

[22] Wang, F-Y. et al (2007). “Social Computing: From Social Informatics to Social Intelligence”, *IEEE Intelligent Systems*, 22(2), 79-83.

[23] White, D., and Rea, A. (2008). “Just Trying to be Friendly: A Case Study in Social Engineering”, *Journal of Information Systems Security*, 4(2), 56-85.

[24] Wulgaert, T., and ISACA (2005). Security Awareness: Best Practices to Secure your Enterprise. IL: ISACA, 2005.

[25] Wolf, M.; Haworth, D.; and Pietron, L. (2011). “Measuring an Information Security Awareness Program”, *The Review of Business Information Systems;* Third Quarter 15(3), 9-21.