Measuring the Effect of Using Simulated Security Awareness Training and Testing on Members of Virtual Communities of Practice

Craig L. Tidwell
Modeling & Simulation, University of Central Florida
Orlando, FL 32816, USA

ABSTRACT

Information security (Infosec) has become a major challenge for all private and public organizations. The protecting of proprietary and secret data and the proper awareness of what is entailed in protecting this data is necessary in all organizations. How does simulation and training influence virtual communities of practice information security awareness over time and with a variety of security scenarios. Can members of a virtual community be significantly changed in how they respond to routine security processes and attempts to breach security or violate the security policy of their organization? How does deterrence play a role in this prevention and education? A study is planned that will train and test users of a virtual community of practice over a 3 month period of time, via a web interface, and using simulated events, to see if the planned security awareness training will be effective in changing their responses to the events and further testing.

Keywords

Communities of Practice
Information Security
Security Policy
Simulation
Virtual Communities

I. INTRODUCTION

We live in an information age that is dominated by virtual communications through such mechanisms as online affinity and network groups (e.g. Facebook, MySpace, Twitter, etc.), virtual online communities, virtual worlds (e.g. Second Life), and other related computer enabled mediation of communication and sharing of knowledge (Wikis, Blogs, etc.). This treatise will focus on security breaches within virtual communities of practice (V-CoP), and will include such areas of security as password creation, data sharing and security, and computer viruses and how they are responsible for massive data losses and untold hours of employee work hours in repairing the damages. In 2003 alone, viruses cost companies an estimated $45 billion (Kjaerland, 2006). The creation of these virtual communities, and the massive amounts of data that are exchanged, managed, and stored in these environments, has posed a predicament for organizations. On one hand, these groups are being leveraged as a new medium for intra – and inter-organizational knowledge sharing. On the other hand, there has never been a more organized underground of computer hackers waiting to take advantage of this target rich environment. Even connections to organized crime have been made by the FBI (Richardson, 2008). Virtualization of communication and sharing of knowledge and data are being handled by many companies through virtual communities that link people together from all parts of the globe.

Balancing the necessity to share information and to control access to this same information has been and will continue to be a challenge among the world's businesses, government agencies, and other organizations. These companies and organizations collect and store a vast quantity of data about their customers, products, employees and partners. Much of these data must be safeguarded and yet still be made available. Cost is the driving factor in this battle, and organizations must balance the costs of securing these data with the costs of losing access to and possession of their information in both quantitative and qualitative terms.

It is difficult to assign specific financial costs to information, but much of the data that is collected and stored by organizations is its lifeblood, and proper protection and security is critical to ensure its continuity and accuracy. In a study conducted by the McAfee Corporation, it is projected that companies worldwide lost more than $1 trillion to computer security breaches in 2008 alone (Knights, 2009). The problem of losses due to hacking has been exacerbated by the current economic downturn, and the study reports that two out of five organizations surveyed were now more vulnerable to breaches. Furthermore, Forrester Research estimates that an average computer security breach can cost a company between $90 and $305 per record (Gaudin, 2007). Since most breaches do not just involve tens or even hundreds of records, but rather hundreds of thousands or even millions of records, the cost of the breach and the cost of repair can be in the millions of dollars. For example, TJX Companies Inc. was hacked in 2007 and a reported 46 to 215 million customer records were stolen (Hakala, 2008). So the cost to TJX could theoretically be as high as $65 billion (215 million records at $305 per record). Questions arise about the causes and remedies of these breaches. In this virtual world of computer transactions, how does an organization adequately protect its valuable information assets?

Organizations all over the world need to learn how to create and implement security policies and procedures to protect organizational data and to make sure that their employees are not only aware of these policies but tested on these policies as part of an ongoing process to ensure that they do not unnecessarily open themselves up to attack. Security

issues are particularly challenging in a V-CoP, where members may be internal employees, external partners, the general public, and even competitors. Users are a large cause of security problems within organizations, and the major cause of most of the worst breaches in 2007 was not from outside hackers, but rather from employees' carelessness (Hakala, 2008).

Furthermore, a large number of information security breaches are caused by human error or human failure when employees fail to follow the specified information security (infosec) policy. Human caused error represents a significant threat, requiring the implementation of controls to reduce the frequency and severity of such mistakes (Whitman, 2004). Lastly, when companies do not meet the specified requirements for data security, whether that shortcoming is willful or negligent, they have failed in their obligations to their stakeholders (Wilson, 2009). Not only is the organization liable to its own internal users but, it is also liable to those parties with a financial interest (e.g. stockholders).

Key to this problem is awareness of security risks and the necessary education and training about information security. Organizations need to increase employee training and awareness to avoid accidental and careless mistakes and to increase the effectiveness of their security policies (Whitman, 2004). Information security awareness can be described as the state where users are aware of, or attentive to, their security mission as expressed in end-user guidelines or the security policy (Siponen, 2000). In the 2009 Computer Security Institute's (CSI)/Federal Bureau of Investigation (FBI) survey, 53 percent of the respondents say that their organizations allocate 5 percent or less of their overall IT budget to information security, and 42 percent spend less than 1 percent of their security dollars on awareness programs which is an alarmingly low expenditure rate when you consider the cost of dealing with security breaches (Richardson, 2008). The fact that approximately $0.50 for every $1,000 is spent on information security reveals the need for more focus on awareness education, training, and continuous and random testing. Simulation can be a cost-effective way to implement a solution to end-user training in proper computer security practices. Included in this simulated training would be a proper understanding of the common security policies that are part of the company's standard operating procedures.

According to Whitman, a security policy is the single most important issue for protecting a computer system or network (Whitman, 2004). Also, Sword and Shield Security Consultants (2001) find the implementation of a security policy as the number one recommended action for protecting an organization's IT systems. The policy should outline both individual and corporate responsibilities, define authorized and unauthorized use of systems, report threats and breaches, and define penalties for violating the policy. The policy should also include a method for updating the policy. Key to these policies is the balance of providing confidentiality, integrity, and availability (Blake, 2000). The cornerstone of the information security policy is ensuring that data are kept private (confidentiality), that the data can be relied upon to be accurate (integrity), and accessible only by authorized (and authenticated) individuals in a timely and available manner. Security policies have long been seen as the key to identifying and managing the security threats and the resources needed to secure information and the systems that hold that data (Anderson, 1996).

In a virtual environment, security poses a serious challenge as part of the problem is the enormous amount of data that are available. Proper utilization and assimilation of collected data can be accomplished through the informal and formal organization of employees in virtual groups that are connected through a shared practice. Such a group, as coined by Wenger and Lave (Wenger, 1999), is called a community of practice (CoP). A CoP is a group of people informally bound together by some shared passion for a joint enterprise (Wenger & Snyder, 2000). A Virtual Community of Practice (V-CoP) is a community of practice that is convened and meets in a virtual environment where members may never meet in person.

Ultimately what is needed is a model that incorporates current security policy models like Bell-Lapuda (Bell, 2005) and Clark-Wilson (Blake, 2000), but incorporates the nuances from a V-CoP where the boundaries, topics of discussion, and membership of the CoP may change on a daily basis (Wenger, 2000). A new model would include a comprehensive security awareness program that incorporates initial training for individuals that are members of a V-CoP and ongoing monitoring and periodic testing. Included with the random testing of members of the V-CoP would be mock security incident testing (Baker, 2008) of the process to make sure that the members are adhering to the security policy they agreed to, are educated about and tested on. Part of this process would be to educate the members of the V-CoP on the potential threats and damages that can be caused by careless behavior that compromises computer security, and may lead to financial and other losses.

The simulated mock security events would be part of the training and would consist of a simulated security incident, such as a counterfeit email, which asks the member of the V-CoP to reveal confidential data or other proprietary information. The member would then have to properly respond to the simulated scenario within the web-based environment. This simulated mock security incidence would be a planned part of the initial training and then would consist of follow-up training events that would occur periodically on an ongoing and irregular basis to test the end-users "awareness" of the security policy. If they do not respond appropriately to subsequent events, they will be presented with follow-up training tips via the web portal to remind them of the security policy. A sufficient passing rate would be determined by the type of organization that the end-user works for and the level of data access associated with the end-user. For example, in a classified environment like military intelligence, or the research and development department of a corporation, the passing rate may be 100%. However, in another environment where the data are not as sensitive, the passing rate could be lower.

II. PURPOSE OF THE RESEARCH

The purpose of this study is to determine and measure the effect that is made on members of a V-CoP when they are provided with security awareness training by means of a simulation on proper security procedures and then presented with several mock security scenarios where they are to apply what they have learned. However, practical security balances the cost of protection and the risk of loss (Lampson, 2000).

Four groups will be used in the study, three control groups (labeled B, C and D), and an experimental group (A). Groups A, B and C will receive a pretest to check their knowledge and understanding of normal security procedures, and more

specifically from a security policy derived from their organization, group D will not. A link to the member of the V-CoP's security policy will be posted so that they can read the policy. Control group B will receive no advanced awareness training but will be presented with the mock security scenarios to see how they respond. Control group C, will receive the initial training but will not receive any further training. The experimental group and control group C will receive the security awareness training, approximately one to two weeks after the pretest and then will be presented with the mock security scenarios/testing. Groups A and B will be evaluated on their responses to the security scenarios/tests and how they fared in relation to the standard procedures and policies of an organization. Approximately 3 weeks after the initial training and test, groups A and B will be presented with another mock security scenario/test and responses will be measured and recorded. The responses will then be compared with the responses recorded in the initial pretest post-test scenario. It is assumed that the users who receive the pre-scenario training will have a higher success rate when responding to the scenario. Users who did not receive the training will respond in a similar manner from the first scenario. Follow up interviews will be performed after the study with subjects where anomalous data is found. For example, if a user does well on the periodic security testing, but still fails to recognize the security compromise attempts, it may be revealing to find out why this happened. Also, data gathered from the tests and events could be presented to the institutions involved to provide feedback on how they may need to change their security policy and procedures.

III. RESEARCH HYPOTHESES

The following are the research hypotheses for the study:

Initial training

Users who receive the security awareness training will show a positive significant difference in how they respond to the post test on computer security in comparison to the users who received no training.

3-weeks after initial training

Users who received the security awareness training will show a positive significant difference in how they respond to mock simulated security events 3 weeks after the training in comparison to the users who received no training.

6-weeks after initial training

Users who received the security awareness training will show a positive significant difference in how they respond to mock simulated security events 6 weeks after the training in comparison to the users who received no training.

9-weeks after initial training

Users who received the security awareness training will show a positive significant difference in how they respond to mock simulated security events 9 weeks after the training in comparison to the users who received no training.

IV. CONCLUSION AND FUTURE WORK

The overarching purpose of this research is to determine the efficacy and sustained benefit of information security awareness training using simulated events in a V-CoP environment. The results of the study would provide useful feedback that organizations can use to determine if awareness training in a web-based simulated environment can help to reduce computer security incidences, particularly from viruses. Proper adherence to security guidelines should help to promote a safer environment. Also, when users are made aware of the risks and potential damages from viruses and other forms of computer security breaches that can occur when these guidelines are not followed, they should be more likely to follow these guidelines. Knowing the risks in any environment is helpful in producing desired responses.

Contributions to the field of computer security could be the longer term impact of training and retraining of members of a V-CoP. This would include the longevity of the training as it relates to retention of information security procedures and policies and the factor of simulated mock incidence events and how these events are handled by users who are exposed to computer security awareness training and users who are not. There has not been enough research into V-CoP and security and this research may lead to further studies being performed.

V. REFERENCES

[1] Anderson, R. (1996): "A Security Policy Model for Clinical Information Systems." IEEE Symposium on Security and Privacy, 1996.

[2] Baker, W., Hylender, C., & Walentine, J. (2008): "2008 Data Breach Investigations Report: A study conducted by the Verizon Business RISK Team." Retrieved from the World Wide Web at http://www.verizonbusiness.com/resources/security/databreachreport.pdf pp. 1-27 on December 10, 2008.

[3] Bell, David (2005): "Looking Back at the Bell-La Padula Model." ACSAC (Annual Computer Security Applications Conference) 2005 proceedings of the 21st ACSAC, Tucson, AZ. IEEE Xplore.

[4] Blake, S. (2000): "The Clark-Wilson Security Model." Indiana University of Pennsylvania, Library Resources. Retrieved from the World Wide Web at http://www.lib.iup.edu/comscisec/SANSpapers/blake.htm, on January 10, 2009.

[5] Gaudin, S. (2007): "Security Breaches Cost $90 To $305 Per Lost Record." Information Week. Retrieved from the World Wide Web at http://informationweek.com/story/showarticle.jhtml?articleid=199000222 on January 12, 2009.

[6] Hakala, D. (2008): "The Worst IT Security Breaches of 2007." IT Security.com. Retrieved from the World Wide Web at http://www.itsecurity.com/features/top-security-breaches-2007-012208/ on March 12, 2009.

[7] Kjaerland, M. (2006): "A taxonomy and comparison of computer security incidents from the commercial and

government sectors." Computers & Security, 2006. Pp 522-538.

[8] Knights, M. (2009): "Security breaches cost $1 trillion last year." ITPro, January 29, 2009. Retrieved from the web at http://www.itpro.co.uk/609689/security-breaches-cost-1-trillion-last-year, on April 12, 2009.

[9] Lampson, B. (2000): "Computer Security in the Real World." Annual Computer Security Applications Conference, 2000, pp 37-46.
Siponen, M., & Oinas-Kukkonen, H. (2007): "A Review of Information Security Issues and Respective Research Contributions." The Database for Advances in Information Systems. Vol. 38, No 1, pp. 60-80.

[10] Wenger, E. (1999): "Communities of practice: learning, meaning, and identity." Cambridge University Press; 1st edition.

[11] Wenger, E. (2000): "Communities of Practice and Social Learning Systems." Sage Publications, Vol. 7(2): pp. 225-246.

[12] Wenger, E. & Synder, W. (2000): "Communities of Practice: The Organizational Frontier." Harvard Business Review, Jan-Feb 2000.

[13] Whitman, M. (2004): "In defense of the realm: understanding the threats to information security." International Journal of Information Management, Vol 24, pp. 43-57.

[14] Wilson, L. (2009, January): "Facing the Information Security Hole in 2009." Retrieved from the World Wide Web at http://www.Information-Security-Resources.com on February 2, 2009.