https://doi.org/10.48009/1_iis_2011_264-270

Issues in Information Systems

Volume XII, No. 1, pp. 264-270, 2011

SECURITY TRAINING HUMAN PROTOCOL

Dr. Harry Benham, Montana State University, hbenham@montana.edu

ABSTRACT

This paper looks at the human side of computer and information security. As it becomes increasingly evident that purely technical procedures and safeguards will not solve computer and information security issues, this paper looks at seven recently identified principles of human psychology that may be exploited to create vulnerabilities. A security training protocol was developed to attempt to explicitly address vulnerabilities arising from these principles. The effectiveness of the human protocol approach was tested on a limited set data. Results of this initial analysis suggest that training of employees using the human protocol approach is more effective than previously used training methods.

Keywords: Security, Learning Styles, User Training, Human Protocol

INTRODUCTION

Computer and information security is universally acknowledged to be critically important. And security demands are increasing. Regulations such as Sarbanes-Oxley, the Health Insurance Portability and Accountability Act, the Gramm-Leach-Bliley Act, European Union Data Protection Directive, and many others require companies to take measures to protect private and personally identifiable information. Some thirty-five states currently mandate notification of individuals in the event that a company experiences a loss of personally identifiable data.

As a result of a few well-publicized data breaches, businesses now recognize that inadequate system security may negatively impact their reputations, market shares, and revenues. As of the writing of this article, the full extent of the breach of Sony's Play Station Network and subsequent loss of customer data is yet to be revealed [15]. Over the years, business organizations have invested heavily in technical safeguards such as firewalls. Yet despite these investments and the considerable efforts of a group of skilled and technically savvy professionals, security threats appear to increase and information losses continue to occur.

In addition to desiring to maintain security, information system managers must also be concerned with the user's level of satisfaction with their systems. Shaw, DeLone, and Niedermann [11] found that data security and privacy had a positive impact on user satisfaction. However several factors related to system usability had a negative impact of user satisfaction lending credence to the popular belief that there is a tradeoff between security and usability [9]. But much of this supposed tradeoff may be due to past emphasis on technical approaches to security.

Yet there is a growing awareness that human elements contribute to computer and information security vulnerabilities [6] [8] [10] [14]. Stanjano and Wilson [12] provide new insights into the nature of human vulnerabilities. This paper looks at the effectiveness of the end-user security training where the training is guided by the vulnerabilities identified by Stanjano and Wilson.

The remainder of this paper is organized as follows. The next section provides a brief literature review. The literature section is followed by a description of the training program initiated and the research hypotheses. The methods and results of that training program will be analyzed and the results of the hypothesis test reported. The final section provides discussion and conclusions.

LITERATURE REVIEW

This brief review is organized into three distinct topic areas: role of human error in computer and information security breaches, human vulnerabilities identified by Stanjano and Wilson [12], and aspects of the vast literature on user training.

Human Error in Security Breaches

Kraemer, Carayon, and Clem [6] assembled focus groups of security practitioners and senior executives from US corporations. These focus groups were tasked with creating causal networks of computer and information security vulnerabilities. These pathways to vulnerabilities all included "Lack of User Training" or "Poor User Support" as contributing to vulnerabilities. More telling was a direct quote from one focus group member blaming security breaches on "stupid people" [6, pg. 518]. Liginlal, Sim, and Khansa [8] used 10 quarters of survey data from Datamonitor reporting on information security breaches and their cause. These data indicated that 64% of the breaches were attributable to human error. From quarter to quarter, the standard deviation for human error as the cause was nearly 20%. These results were consistent with a number of pervious studies cited. Thus, there is empirical evidence suggesting that human error is a significant source of security breaches. Additional support for the importance of human behavior can be found in Dhillon and Torkzadeh [3].

Gross and Rosson [4] acknowledge that human users are involved in security breaches, but they contend that the users are agents of their organizations with sophisticated strategies regarding sensitive data. The problem, in their estimation, is that security professionals have failed to consider how users view security. A similar theme is found in Parkin, van Moorsel and Coles [10] who argue that security managers often regard human behavior as a liability when they should accommodate human behavior as a part of their security management procedures.

Möller *et.al.* [9] developed a probabilistic and rule driven simulation for how users would react to security practices and procedures. They then compared actual user behavioral responses to the model's prediction and found a good deal of agreement. Their point is that user behavior is predictable in security-relevant situations and that therefore security procedures should be designed to account for this predictable user behavior.

Two sets of authors have attempted to classify users into groupings that would facilitate predicting user hehavior in security-relevant situations. Stanton *et.al.* [14] classify users by Expertise and Intentions. Expertise has two levels, High and Low, while Intentions has three levels, Beneficial, Neutral, and Malicious. They then identify each cell in their two by three grid, provide a label for the cell, and descriptive behaviors. Alfawaz *et.al*. [1] produce a two by two classification based on Skill and Knowledge. For each of the four modes in their classification, they establish behavioral scenarios. These classification schemes and their corresponding prescriptions are not particularly useful.

Human Vulnerabilities

Stanjano and Wilson [12] [13], first in a working paper and more recently in a published article, identify seven principles of human behavior they believe to be relevant to system security. Their seven principles were derived for an extensive analysis of scams conducted by con artists. These scams, in one version or another, have been used successfully for generations. Thus the principles derived from analysis of these scams are claimed to represent aspects of human psychology that can be exploited. Stanjano and Wilson argue that computer security engineers must understand the implications of these principles and design their security systems according. Their seven principles are:

1. Distraction Principle: While user is focused on whatever has their attention, hustler can do anything and it will not be noticed.
2. Social Compliance Principle: People are socialized to not question authority. A fraudster can feign authority to gain cooperation.
3. Herd Principle: Naturally suspicious individuals let down their guard when everyone appears to share the same risks.
4. Dishonest Principle: Our inner larceny gets us to participate in shady deals – and then not report them when it turns out to be a fraud.
5. Kindness Principle: People are fundamentally nice and willing to help.
6. Need and Greed: Our needs and desires make us vulnerable and easily manipulated.
7. Time Pressure: Under time constraints, decision strategies become more heuristic and less carefully reasoned.

Most scams make use of several principles simultaneously. Consider an email message apparently from your e-mail administrator informing you that your mail disk-quota has been exceeded and directing you to immediately provide your user credentials or you'll lose your email privileges. This scenario is making use of three principles. First, Social Compliance as it appears to come from your e-mail administrator – a person of some authority. Second, Distraction as it is hoped that you'll focus your attention on preserving your valuable email. And third, there is Time Pressure. How can security personnel design against this type of attach? In military contexts, making potentially critical decisions under time pressure have been dealt with by establishing "human protocols" to enforce step-by-step rational checks. User training focusing on pre-scripted "human protocols," may be one approach to dealing with scenarios like this.

User Training

The literature on user training is extensive and no attempt at a comprehensive summary will be made. Rather two points will be made from the literature. First, Bostrom *et.al.* [2] established that learning styles are important in the training of end-users. Kolb's [5] Learning Style Inventory provides a method for measuring learning styles. Kolb's learning styles are based on a theory that postulates that individuals learn and solve problems by progressing through a four-stage cycle: concrete experience (CE) followed by reflective observation (RO), which leads to the formation of abstract concepts (AC), which in turn lead to the testing of hypotheses through active experimentation (AE). The cycle repeats. Learners develop preferences for a particular stage.

Kolb views AE and RO as being at opposite ends of a continuum of active involvement in learning. The same is the case with AC and CE being opposite ends of a continuum from abstract to concrete. By combining the AE – RO scale and the AC – CE scale into a coordinate system, four learning styles are defined by the four quadrants.

Second, security training can be effective. Kumaraguru *et.al.* [7] considered three methods for training users to recognize phishing attacks. The first method was to simply direct users to online resources provided by eBay or the FTC for example to "educate" users about phishing. Their second method was to periodically send phishing emails to users and make use of the teachable moment when a user fell for the phishing. Their final method was the development of an interactive game for recognizing phishing attacks. Simply viewing online resources was not effective. But both the "training" phishing emails and particularly the video game, were effective in reducing the frequency of successful phishing attacks fell.

TRAINING PROGRAM

The security officer for a local, security conscious employer attempts to provide regular security training for all users. Their training consisted of providing users with a list of potential security threats along with the usual recommendations such as "Never open an attachment from an unknown source" and "Disable ActiveX, Flash, and Javascript from untrusted sites." The security officer's intuition was that these admonitions were minimally effective but better than nothing. This security officer was intrigued by the potential for using Stanjano and Wilson's seven principles.

Developing a Security Training Human Protocol

Stanjano and Wilson's Time principle comes with the observation that "human protocols" have been used successfully by military organizations for dangerous situations that require rapid response. Furthermore, many computer and information security threats try to exploit the time principle. Therefore, it was decided to develop a human protocol to use for security training.

The human protocol is essentially to walk through the other six principles for fact checking. The protocol first calls for a distraction fact check. In the e-mail disk quota exceeded scenario mentioned earlier, the protocol would direct the user to check the facts. Is the name of the email in the message the name of the email program being used? Is there an email disk quota? How much space am I using?

To break the Social Compliance Principle, the protocol calls for users to challenge authority. The security officer agreed that all communication would include the full name of the sender. The protocol instructs users to verify the authority by checking with the security officer if there is any doubt.

The Herd Principle's protocol asks users to question their assumptions. Does the fact the sites such as Facebook have attracted millions of users demonstrate that its privacy protections are adequate?

The protocol for the Dishonesty principle was to explicitly offer immunity for the first 'dishonest' incident provided the user cooperates with any forensic investigation. The idea here is that quickly discovering the extent and severity of any incident is more important than punishing an individual employee.

Finally protocols for the Kindness Principle and the Need and Greed Principle ask the user to question the veracity of what is being presented. Would a disaster victim truly have such a story? Can you verify the story independently? Is it reasonable to expect true love to follow from an unknown "I Love You" email message.

The training program consisted of presenting users with a number of scenarios created to closely resemble real threats and have the users practice applying the protocol.

Hypothesis Generation

The obvious hypothesis to test is whether or not security training using scenarios and the human protocol was effective.

H1: Employees trained using the human protocol experienced fewer computer and information security incidents than traditionally trained employees.

As discussed below, our data comes from an organization that switched from traditional security training to human protocol security training. The most recently trained employees had the human protocol training. To attempt to distinguish the effect of human protocol training from time since training, we introduce the following hypothesis based on the assumption that training is likely to be most effective immediately after it is received.

H2: Security Training effectiveness will diminish over time.

Any computer training is a learning experience for the individuals being trained. Those individuals will have different learning styles. Following Bostrom et.al. [2] where training was more effective for learners who's preferred style favored abstract concepts and for learners who's preferred style favored more active experimentation we have the following two hypotheses.

H3: Security Training will be more effective for learners who score higher on the AC – CE scale.

H4: Security Training will be more effective for learners who score higher on the AE – RO scale.

METHODS

The company provides security training each quarter to roughly one quarter of their employees. We now have two quarters of detailed record keeping. The distribution of employee's trained, training method, and time since training is shown in Table I.

TABLE I

Quarters Since Training	Human Protocol Training	Traditional Training
0	65	0
1	35	29
2	0	61
3	0	59

Kolb's learning style inventory is routinely administered to all employees at the time of hire. Thus scores on Kolb's AC-CE scale and AE – RO scales are available. To measurement training effectiveness, all user security incidents were monitored for 30 days following completion of training. When the first human protocol cohort was trained, three other traditionally trained cohorts were also monitored. When the second human protocol cohort was trained, the initial human protocol cohort was again monitored as well as the remaining two traditionally trained cohorts. A security incident was defined to be any activity which could potentially have lead to a computer or information security breach. For example, it would be considered a security incident if a user caused unencrypted sensitive data to be stored on a laptop computer even though no actual harm resulted. That user's actions created a potential for a data breach. Security incidents were infrequent. Each employee's training effectiveness was coded as a 0 if there was a security incident involving the employee during the 30 day monitoring. Otherwise, an employee's training effectiveness was coded as a 1.

With a dichotomous measure of training effectiveness, an appropriate empirical technique would be one of the limited dependent variable "regression" techniques such as a logistic regression. For those unfamiliar with logistic regression, the functional specification sets the dependent variable to be the natural logarithm of the odds of observing a 0 or 1 using a logistic probability distribution. Independent variables influence the shape of the probability distribution. One way to characterize logistic regression models is as estimating the probability of observing a 1. There are a few changes in terminology from standard linear regression. Independent variable effects are estimated rather than parameter values. Maximum likelihood estimation is used. Significance of independent variable effects are calculated as is a pseudo R-Square measure to judge overall model fit.

RESULTS

Table II displays the results of a logistical regression run using training effectiveness as the dependent variable. Training type is a categorical variable. Table II lists Human Protocol only as the traditional training method is left out as a reference group. Thus the Human Protocol effect is relative to traditional training. Since it is not reasonable to believe that the decay rate of training is linear, quarters since training are treated as categorical variables with the reference group being the 0 indicating training in the current quarter. Learning style measures of Kolb's Abstract – Concrete (AC – CE) and Active – Passive (AE-RO) scales are in included in the logistical regression as controls. Results are shown in Table II.

TABLE II

Training Effectiveness		
Variable	**Effect**	**Significance**
Human Protocol	0.0412	0.035
Quarters Since Training		
1	-0.0044	0.126
2	-0.0060	0.113
3	-0.0144	0.073
4	-0.0161	0.048
Kolb: AC - CE	0.0242	0.046
Kolb: AE – RO	0.0339	0.062
Pseudo R-Square	0.417	

Hypothesis 1 appears to be supported. The positive estimated effect for human protocol training indicates that the probability of an employee trained with the human protocol approach not experiencing any security incidents is significantly higher than the probability that a similar employee who's received the company's traditional security training. The reported significance, the probability that the variable has no measurable effect, is 0.035, well within the customary 5% significance standard.

The consistent negative signs on the number of quarters since the employee received security training indicate that the effectiveness of training diminishes over time. One can observe that the magnitude of the effect increases as the time since training increases. However, the quarters since training effect is significant only for those trained 4 quarters ago, and then the significance of the effect just comes in under the traditional 5% standard. The results are suggestive of support for Hypothesis 2: training effectiveness diminishes over time. But with only one measured effect statistically significant, the evidence supporting Hypothesis 2 is relatively weak.

Hypotheses 3 and 4 are included to control for individual differences. Table II suggests that employees with a stronger preference for abstract conceptualization are less likely to experience a security incident (e.g. their security training was more effective). At a 5% significance level, the null hypothesis of no measureable effect would be rejected. Similarly, Table II suggests that employees with stronger active experimentation learning preferences are less likely to be involved in a security incident. The active experimentation effect, however, was not significant at a 5% significance level.

The pseudo-R-Square statistic indicates that approximately 42% of the variation in the effectiveness of security training can be explained by training type, quarters since training occurred, and individual learning style. While 42% explained means that 58% remains unexplained, 42% explained variation in what is essentially a cross-sectional analysis is reasonably good. From Table I, it is clear that the numbers involved in the analysis are not large.

DISCUSSION

There is a confounding influence that makes it more difficult to interpret the human protocol training type effect reported in Table II. As the employer totally switch training type to human protocol training and data collection did not begin until after the first human protocol cohort was trained, it is difficult to completely distinguish between time since training and the impact of human protocol training. Inclusion of the time since training attempts to distinguish between the human protocol training length of time since training. However, there are no observations for training effectiveness for traditionally trained employees immediately after the completion of training. Thus the possibility remains that some of the observed human protocol training effect is confounded with the recency of training.

Table II shows a clear pattern of the effects of security training atrophing over time. The employer, by insisting upon annual security training, exhibits a belief that either the security landscape changes very rapidly or employees' security awareness decays over time. Seeing the pattern gives some hope that we were able to distinguish between the human protocol effect and time since training. The lack of significance could be due to covariance between training type and time since training variables.

It is interesting to note that Bostrom *et.al.* [2] found that the abstract conceptualization effect was larger than the active experimentation effect. In this study the magnitudes are reversed. In Table II, training appears to be more effective for those with higher active experimentation than those with higher abstract conceptualization. Recall that the estimated active experimentation effect was not statistically significant.

CONCLUSION

Computer and information security matters. It is becoming increasingly evident that purely technical procedures and safeguards will not suffice. This paper utilized seven recently identified principles of human psychology that may be exploited to create vulnerabilities. Rather than rile against users ill judged behavior, security professionals should acknowledge human vulnerabilities and consider create a human protocol security training approach to minimize the acknowledged risks.

With a single employer study and limited long-term data available, the results reported in Table II suggest that the training approach taken in this paper could potentially be effective.

REFERENCES

1. Alfawaz, S., K. Nelson, & K. Mohannak (2010). Information Security Culture: A Behaviour Compliance Conceptual Framework. *Proceedings, 8th Australasian Information Security Conference (AISC 2010).* Brisbane, Australia.
2. Bostrom, R., L. Olfman, & M. Sein. (1990). The Importance of Learning Style in End-User Training. *MIS Quarterly*. 15(1): 101-119.
3. Dhillon, G. & T. Torkzadeh. (2006). Value-Focused Assessment of Information System Security in Organizations. *Information Systems Journal*, 16:293-314.
4. Gross, J., & M. Rosson. (2007). Looking for Trouble: Understanding End-User Security Management. *Proceedings, Computer Human Interaction for Management of Information Technology (CHIMIT '07).* Chambridge, MA, USA.
5. Kolb, D.A. (1976). *The Learning Style Inventory Technical Manual*, McBer and Company, Boston, MA, 1976.
6. Kraemer, S., P. Carayon, & J. Clem. (2009). Human and Organizational Factors in Computer and Information Security: Pathways to Vulnerabilities. *Computers & Security*. 28(3):509-520.
7. Kumaraguru, P., S. Sheng, A. Acquisti, L. Cranor, & J. Hong. (2010). Teaching Johnny Not to Fall for Phish. *ACM Transactions on Internet Technology.* 10(2):7.1-7.31.
8. Liginlal, D., I. Sim, & L. Khansa. (2009). How Significant is Human Error as a Cause of Privacy Breaches? An Empirical Study and a Framework for Error Management. *Computers & Security*. 28(1): 215-228.
9. Möller, S., N. Ben-Asher, K. Engelbrecht, R. Englert, & J. Meyer. (2011). Modeling the Behavior of Users Who Are Confronted with Security Mechanisms. *Computers & Security*. 30(2): 242-256.
10. Parkin, S., A. van Moorsel, & R. Coles. (2009). An Information Security Ontology Incorporating Human-Behavioural Implications. *Proceedings, 2nd International Conference on Security of Information and Networks (SIN'09*), North Cyprus, Turkey.
11. Shaw, N., W. DeLone, & F. Niederman. (2002). Sources of Dissatisfaction in End-User Support: An Empirical Study. *Data Base*. 33(2):41-56.
12. Stanjano, F. & P. Wilson. (2009). *Understanding Scam Victims: Seven Principles for Systems Security*. Technical Report UCAM-CL-TR-754. University of Cambridge Coomputer laboratory, Cambridge, UK.
13. Stanjano, F. & P. Wilson. (2011). Understanding Scam Victims: Seven Principles for Systems Security. *Communications of the ACM.* 54(3):70-75.
14. Stanton, J., K. Stam, P. Mastrangelo, & J. Jolton. (2005). Analysis of End User Security Behaviors. *Computers & Security*. 24(1):124-133.
15. Thomas, K. (2011). Sony Makes It Official: PlayStation Network Hacked. *PcWorld.* April 23, 2011.