Measuring An Information Security Awareness Program

Michael Wolf, University of Nebraska at Omaha, USA
Dwight Haworth, University of Nebraska at Omaha, USA
Leah Pietron, University of Nebraska at Omaha, USA

ABSTRACT

Research shows security awareness lacks a uniform definition. This paper explores the various attempts that have been made to define security awareness and then presents a clear and concise definition of security awareness. Due to the lack of a behaviorally-oriented measurement, security awareness has relied on the use of self-reported questionnaires and surveying users through this same type of instrument. These attempts assume that knowledge of security awareness leads to correspondingly correct behavior, without attempting any field validation that this paradigm holds true. This paper goes beyond self-reporting and measures the behavior of end-users. It compares that behavior with policy to determine the actual compliance percentage and draws conclusions from these results.

Keywords: security; security awareness; passwords; behavioral measurement

INTRODUCTION

Previous research examining security awareness effectiveness has shown inconclusive results. At the end of his study, Decker (2006, p. 49) states that there is no correlation between security awareness training and compliance with policy. These inconclusive and unreliable results derive directly from the lack of a clear and concise definition of security awareness.

Measurement in previous research has been attempted largely through the use of self-reporting surveys/questionnaires and through quizzes of end-users' knowledge. These attempts assume that knowledge of security awareness equates to the correct behavior by the end-user. These attempts have not evaluated actual end-user behavior. This paper evaluates the actual security behaviors of end-users and how the interventions applied affect their behavior.

LITERATURE REVIEW

Security Awareness Definitions

Awareness is the basis for information security programs; by making users aware of security issues, users are better able to protect not only themselves but the organization as a whole. McCumber states that "education, training and awareness may be our most prominent security measures" (2005, p. 106). Although McCumber (2005, p. 106) states that awareness is an important part of any organization's security program, he fails to define what awareness is and how awareness can impact an organization, only stating that it is important and needed.

Okenyi and Owens state that security awareness "brings about behavioral change," which is the component of the awareness definitions that Siponen (2000), Rudolph (2009), Willett (2008), Hansche (2001a) and Krutz and Vines (2001) leave out (2007, p. 302). On the other hand, Okenyi and Owens (2007) fail to discuss the knowledge portion of security awareness.

NIST Special Publication 800-50 adds a more concise view that "security awareness efforts are designed to change behavior or reinforce good security practices" (2003, p. 8). According to NIST (NIST SP800-50, 2003, p. 8), a security awareness program's first objective is to disseminate information to individuals about information security-related topics. The program must be structured in a way that changes both the individual's perceptions and behavior, thus increasing the likelihood that when a security event happens, the appropriate response will occur (NIST SP800-16-Rev1, p. 15, 2009; NIST SP800-50, 2003, p. 8).

Security awareness contains two equally important pieces. The first piece is the dissemination of accurate, current and appropriate knowledge of policy to individuals. Policies explain to individuals the threats they need to be cognizant of as well as the appropriate actions to take upon encountering a threat. The second portion of awareness is the delivery of policy in a manner that convinces an individual to change his or her behavior. These two portions are equally important; without one, the other is ineffective.

A number of academic studies suggest that additional research is needed in the area of security awareness; Tsohou, Kikilakis, Karyda and Kiountoizis state that their "analysis reveals that security researchers, practitioners and managers may be frustrated with security awareness efforts, since there is no clarification of many issues of concern" (2008a, p. 225). Tsohou, et. al., elaborate some of the "issues of concern" in information security awareness as:

1. terminology ambiguity;
2. "the study of applied methods of ISA [Information Security Awareness] reveals that most research approaches are not theoretically grounded;"
3. "no common understanding of the security awareness ultimate goal;"
4. "very often methodologies employed to achieve it [awareness] are, at best, not suitable;"
5. "most approaches focus only or mostly on product aspects of ISA; an obstacle in revealing critical aspects of the process that could lead us in explaining the reasons why security awareness attempts may fail" (2008a, p. 225).

Tsohou, et. al., go on to recommend that "the investigation of the identified ambiguous issues (e.g., the roles allocated to information security stakeholders, the enablers and inhibitors of security awareness success) in organizational settings" are valid areas of future research (2008a, p. 225).

There is a need for a clear and concise definition of security awareness. Based upon the foregoing discussion, this paper proposes that *security awareness is the effort to impart knowledge of or about factors in information security to the degree that it influences users' behavior to conform to policy.*

Purpose Of The Study

The purpose of this paper is to create and validate the proposed definition by applying it in field research. The research setting is a K-12 organization that is trying to improve compliance with password policy. Based upon the new definition, four different password policy interventions were applied. The behaviors of the end-users were then examined to determine if their passwords meet the password complexity requirements.

HYPOTHESES

The following hypotheses are evaluated in this paper:

1. There will be a measurable difference between the pretest and posttest results for each intervention performed.
2. There will be a diminishing change as a result of each intervention following the first intervention.

METHODOLOGY

Research Group

The research group consisted of 122 adults. These adults included all positions, including teachers, custodians, maintenance personnel, residential staff, business office staff and bus drivers.

Research Design

The experiments followed The One-Group Pretest-Posttest Design as outlined by Cook and Campbell (1979, p. 99). A single group of individuals consisting of faculty and staff at a K-12 school were selected as the test population. A pretest was done to determine the rate of compliance of the population with the school's computer password policy.

Measurement

To test the compliance, the password hashes were first extracted from the school's user accounts on one of the active directory domain controller servers. For a password to be considered compliant, the password must meet the following conditions, as defined by the educational institutions password policy:

1. Passwords must be changed every 180 days;
2. All passwords must be at least eight characters in length;
3. All passwords must contain three of the following four types of characters:
    a. upper case letter,
    b. lower case letter,
    c. numerical character, and
    d. a special character (those ASCII characters such as !@#$%).

The second requirement of the password policy, password length, was enforced through an Active Directory Group Policy.

To test the actual passwords, the following steps were performed. Using a command prompt, the following command was executed: pwdump3e.exe DC_NAME results.txt, where DC_NAME is the name of the domain controller that the utility will use to extract the text file of password hashes. This file was moved to a workstation for further evaluation. A program named RainbowCrack was used to determine the password values (RainbowCrack Project, 2010). The results were imported into Excel 2007 as a baseline. With the baseline established, four interventions were developed and delivered over a six-week period to determine their effectiveness on raising the compliance rate.

The first intervention performed was a live presentation given to all staff members during in-service week. The presentation began with a refresher of the password policy that had been in place since 2007 and an explanation of why this policy was in place. The presentation included the characteristics of good and bad passwords. The entire presentation, which included a question and answer period, was twenty-two minutes.

The second intervention occurred two weeks later in the form of an e-mail sent to staff members. This e-mail contained a reminder on the complexity requirements, the length, and the requirement for changing passwords every 180 days. The e-mail concluded with a link to the web-based password management program.

The third intervention was a popup box that appeared when staff members logged into their computers. This popup asked the staff member who had logged on if he or she had changed his or her password lately. Staff members had to click OK to clear the popup message to logon to the computer. This popup box was enabled for four days.

The fourth and final intervention consisted of a poster campaign. Indiana University provides blank posters on their website (http://informationpolicy.iu.edu/education/downloads.shtml#ncsam05) for use by the general public with the requirement that the Indiana University copyright be maintained on the bottom of the poster. A poster was used for the fourth intervention and modified to ask the question "Have you changed your password lately?" The posters were printed and placed on informational bulletin boards in thirteen campus locations. These posters were left up for one week.

Interventions one and two were allowed to run for two weeks before the next intervention was applied, thereby allowing adequate time to pass for the intervention to take effect. The third and fourth interventions were applied for one week. At the end of each day during the experiment, the password hashes for all staff members were extracted to a text file to allow for longitudinal comparison of the interventions. The data were aggregated to show the overall compliance for the school over time and the effectiveness of each intervention.

FINDINGS

Initial Results

A password dump was performed immediately before the first intervention to establish a baseline compliance percentage. For the 122 accounts that were tested, the initial baseline compliance was forty-four percent. When the rate of compliance for password complexity is examined, four percent of the total passwords used all four types of characters, capital letters, lower case letters, numerical characters and special characters; forty percent used three of the four types of characters; forty-eight percent used two of the four types of characters, and eight percent used a single type of character.

First Intervention

Two weeks was given for the staff to make any changes to their passwords. As indicated in Figure 1, immediately after the intervention compliance rose to forty-nine percent and increased to fifty percent the following day. After the first week, compliance had risen to fifty-five percent. However, after the first week, the number of compliant passwords did not change for the remainder of the period.

The McNemar Test for Significance of Changes was calculated for the first intervention using the initial pretest results and the final posttest result. The H_0 for this test is that the password compliance has not been altered. The H_1 for this test is that the password compliance has been altered. A value of one was assigned to those accounts that had a password that was compliant. A value of zero was assigned to those accounts that had a password that was not compliant. Figure 2 contains the contingency table and calculations for the first intervention. Based upon these results, Hypothesis H_0 is rejected. Hypothesis H_1 is accepted, there was a statistically significant change between the pretest and posttest results. In this particular intervention, the number of compliant passwords rose.

Second Intervention

The second intervention was an e-mail sent to all staff members on August 25, 2010. As indicated in Figure 3, it took three days for there to be a change in the number of compliant passwords. Compliance did rise to fifty seven percent. Compliance stayed at fifty seven percent through the remainder of the two week period.

The McNemar Test for Significance of Changes was calculated for the second intervention using the initial pretest results and the final posttest result. The H_0 for this test is that the password compliance has not been altered.

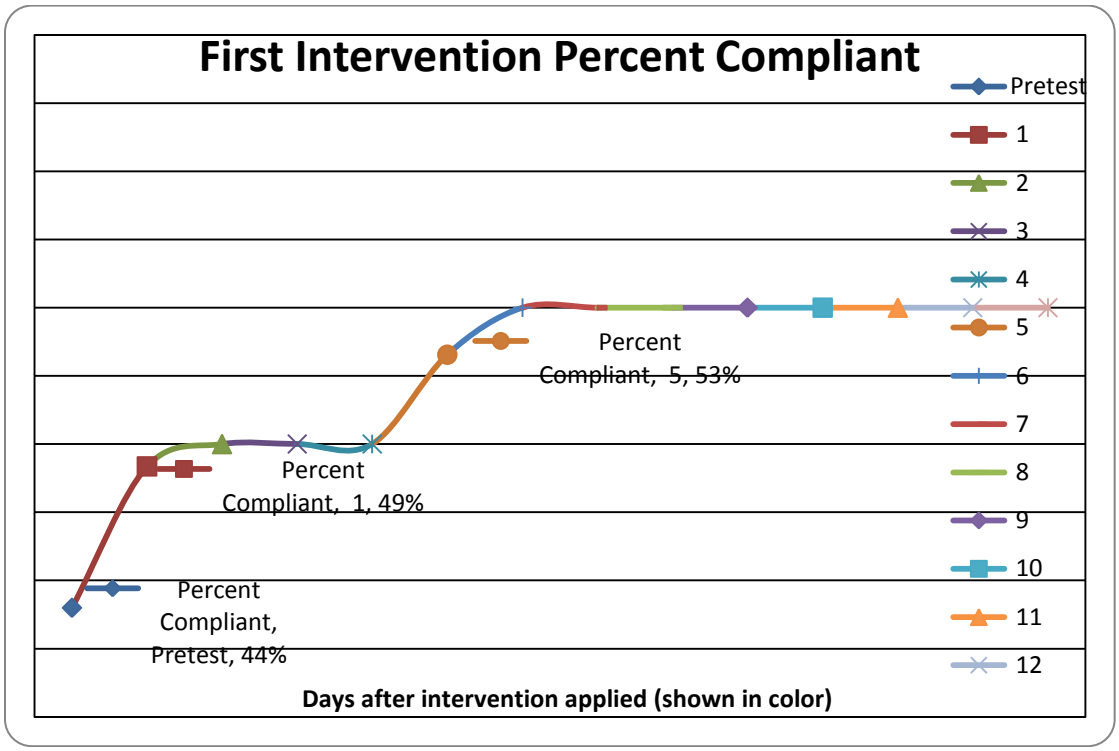

Figure 1: Percentage Of Compliant Passwords For The First Intervention.

McNemar Test for Significance of Changes for the First Intervention

		Classification of the Y_i		
		$Y_i = 0$	$Y_i = 1$	X = Pretest
Classification	$X_i = 0$	56	12	Y = Posttest
of the X_i	$X_i = 1$	0	54	0 = Not Compliant
				1 = Compliant
Test Statistic	T_1=	$\frac{144}{12}$=12		
	T_2 =	12		
		T_1	**T_2**	
		n=12	n=12	
		p=.5	p=.5	
		α=.025	α=.05	
		y=2	y=3	

D_1: T_2 not less than or equal to y, do not reject H_0
D_2: $T_2 \geq$ 12-3, reject H_0
*Reject H_0, Accept H_1 -> password compliance HAS been altered

Figure 2: McNemar Test For Significance Of Changes For First Intervention

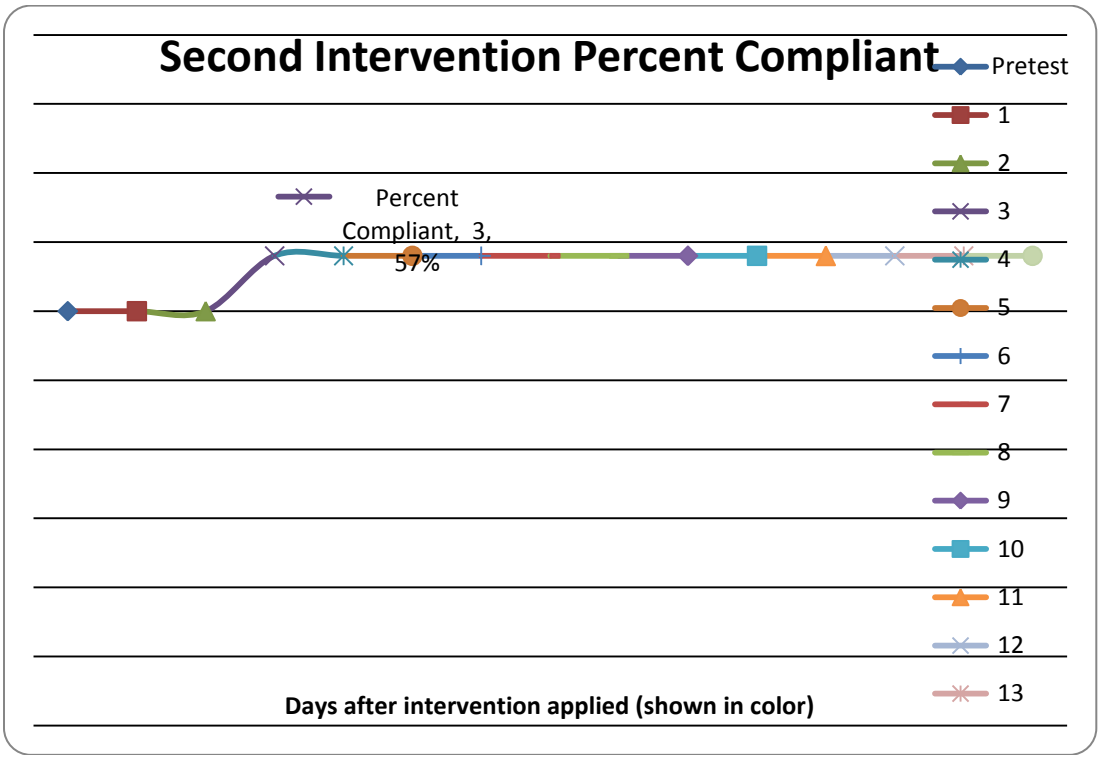

Figure 3: Percentage Of Compliant Passwords For The Second Intervention

McNemar Test for Significance of Changes for the Second Intervention

		Classification of the Y_i		
		$Y_i = 0$	$Y_i = 1$	X = Pretest
Classification	$X_i = 0$	53	3	Y = Posttest
of the X_i	$X_i = 1$	0	66	0 = Not Compliant
				1 = Compliant
Test Statistic	T_1=	9 =3		
		3		
	T_2 =	3		
		T_1	**T_2**	
		n=3	n=3	
		p=.5	p=.5	
		α=.025	α=.05	
		y=0	y=0	

D_1: T_2 not less than or equal to y, do not reject H_0
D_2: $T_2 \geq 3\text{-}0$, reject H_0
*Reject H_0, Accept H_1 -> password compliance HAS been altered

Figure 4: McNemar Test For Significance Of Changes For Second Intervention

The H_1 for this test is that the password compliance has been altered. A value of one was assigned to those accounts that had a password that was compliant. A value of zero was assigned to those accounts that had a password that was not compliant. Figure 4 contains the contingency table and calculations for the second intervention. Based upon these results, Hypothesis H_0 is rejected. Hypothesis H_1 is accepted, reporting that there was a statistically significant change between the pretest and posttest results. In this particular intervention, the number of compliant passwords rose.

Third Intervention

The third intervention was a login popup box enforced through Active Directory Group Policies. This popup box was displayed for four days. The overall compliance level rose by one percent to fifty-eight percent during this time period. This increase can be seen in Figure 5.

The McNemar Test for Significance of Changes was calculated for the third intervention using the initial pretest results and the final posttest result. The H_0 for this test is that the password compliance has not been altered. The H_1 for this test is that the password compliance has been altered. A value of one was assigned to those accounts that had a password that was compliant. A value of zero was assigned to those accounts that had a password that was not compliant. Figure 6 contains the contingency table and calculations for the third intervention. Based upon these results, Hypothesis H_0 is rejected. Hypothesis H_1 is accepted, reporting that there was a statistically significant change between that pretest and posttest results. In this particular intervention, the number of compliant passwords rose.

Fourth Intervention

The fourth and final intervention was a Halloween themed poster campaign. After being posted in staff areas, the posters were left up for one week. The overall compliance rose by two percent to a total of sixty percent compliant in the first two days of the poster campaign, as indicated in Figure 7.

The McNemar Test for Significance of Changes was calculated for the fourth intervention using the initial pretest results and the final posttest result. The H_0 for this test is that the password compliance has not been altered. The H_1 for this test is that the password compliance has been altered. A value of one was assigned to those accounts that had a password that was compliant. A value of zero was assigned to those accounts that had a password that was not compliant. Figure 8 contains the contingency table and calculations for the third intervention. Based upon these results, Hypothesis H_0 is rejected. Hypothesis H_1 is accepted, reporting that there was a statistically significant change between that pretest and posttest results. In this particular intervention, the number of compliant passwords rose.

Final Results

Upon the completion of four interventions, the overall percentage of compliant passwords rose from forty-four percent to sixty percent. A longitudinal representation of the overall increase in password complexity compliance is shown in Figure 9. This longitudinal representation shows the overall rise in password complexity compliance through the four interventions.

DISCUSSION

Each intervention, demonstrated an increase in the number of passwords that met the complexity requirements of the school. These results confirm that Research Hypothesis 1, that there will be a measureable difference between the pretest and posttest for each intervention, can be accepted. The compliance percentage for the passwords increased fourteen percent after the first intervention. However after the first intervention, the percentage increases dropped to one or two percent for interventions two, three and four. These results suggest that Research Hypothesis 2, that there will be diminishing effects after the first intervention, can be accepted.

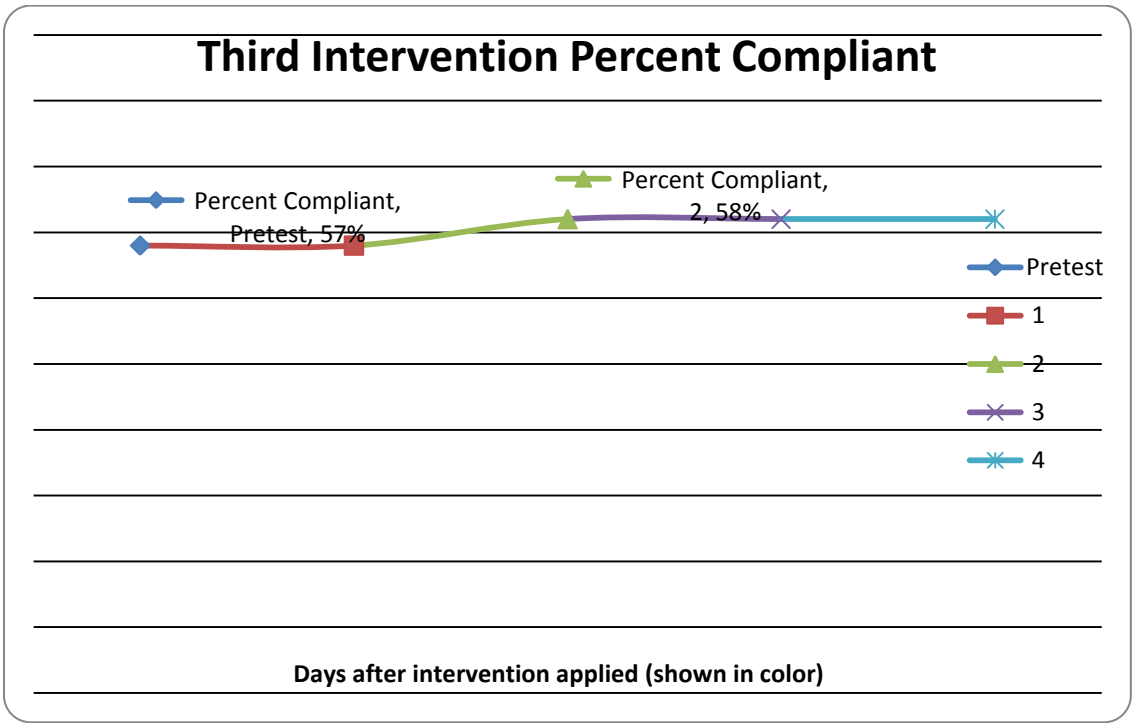

Figure 5: Percentage Of Compliant Passwords For The Third Intervention.

McNemar Test for Significance of Changes for the Third Intervention

		Classification of the Y_i		
		$Y_i = 0$	$Y_i = 1$	X = Pretest
Classification	$X_i = 0$	52	1	Y = Posttest
of the X_i	$X_i = 1$	0	69	0 = Not Compliant
				1 = Compliant
Test Statistic	T_1=	$\frac{1}{1} = 1$		
	T_2 =	1		
		T_1	**T_2**	
		n=1	n=1	
		p=.5	p=.5	
		α=.025	α=.05	
		y=0	y=0	

D_1: T_2 not less than or equal to y, do not reject H_0
D_2: $T_2 \geq 1\text{-}0$, reject H_0
*Reject H_0, Accept H_1 -> password compliance HAS been altered

Figure 6: McNemar Test For Significance Of Changes For Third Intervention

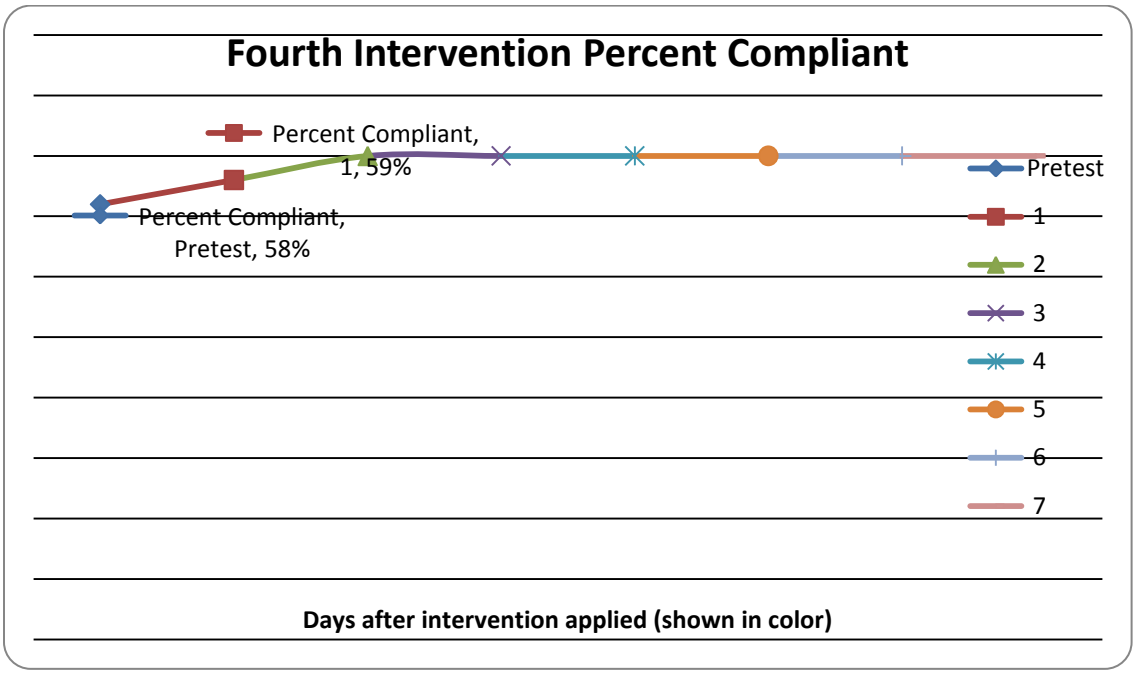

Figure 7: Percentage Of Compliant Passwords For The Fourth Intervention.

McNemar Test for Significance of Changes for the Fourth Intervention

		Classification of the Y_i		
		$Y_i = 0$	$Y_i = 1$	X = Pretest
Classification	$X_i = 0$	49	3	Y = Posttest
of the X_i	$X_i = 1$	0	70	0 = Not Compliant
				1 = Compliant
Test Statistic	T_1=	9 = 3		
		3		
	T_2 =	3		
		T_1	**T_2**	
		n=3	n=3	
		p=.5	p=.5	
		α=.025	α=.05	
		y=0	y=0	

D_1: T_2 not less than or equal to y, do not reject H_0
D_2: $T_2 \geq$ 3-0, reject H_0
*Reject H_0, Accept H_1 -> password compliance HAS been altered

Figure 8: McNemar Test For Significance Of Changes For Fourth Intervention

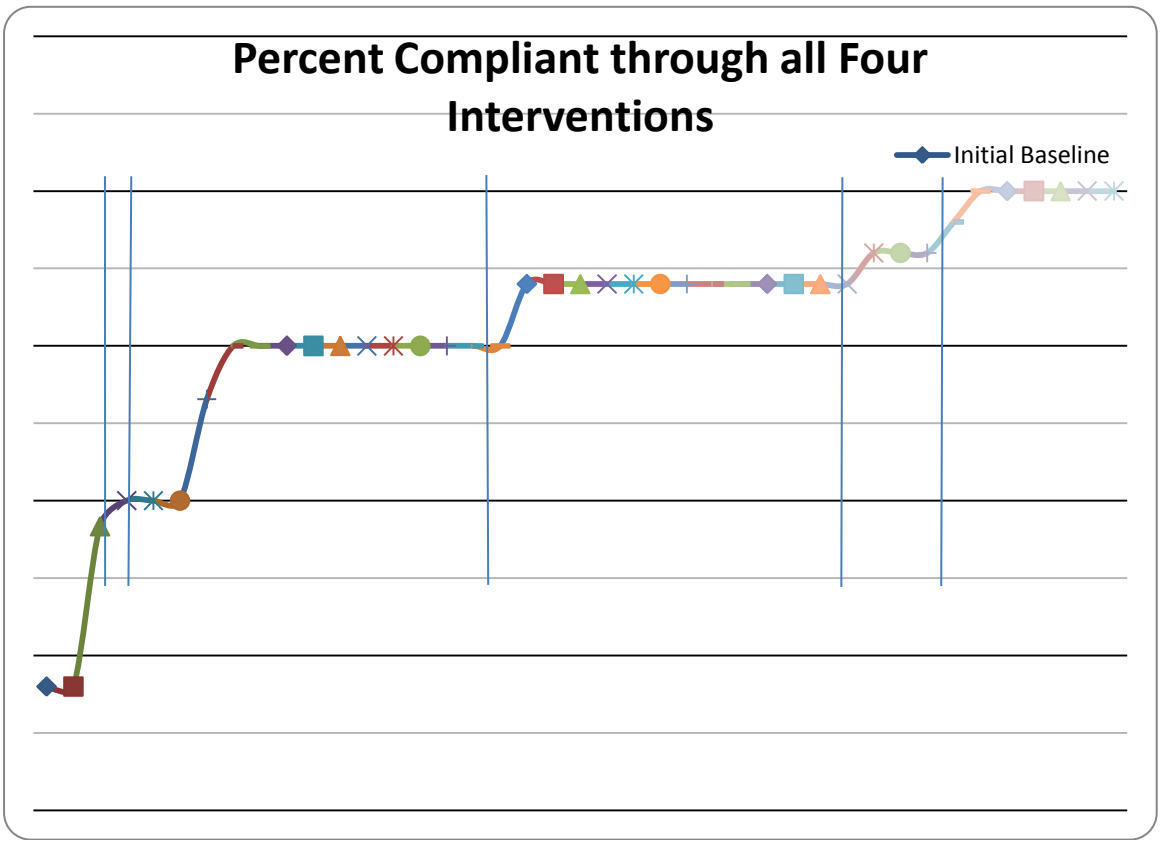

Figure 9: Percent Compliant Over All Four Interventions.

With regard to the first hypothesis, the results show that all interventions had a statistically significant positive impact on the compliance level. The first intervention had the largest impact. Interventions two, three and four had measureable impacts but they were practically inconsequential.

The second hypothesis, is there a point at which interventions begin to lose their effectiveness, appears to be yes. The first intervention had the greatest impact. The second, third and fourth interventions had a significantly lower impact on the overall compliance percentage. The overall graphical representation shows an "S" curve with a flattening of the curve following the first intervention. This flattening could be for a number of reasons including: the first intervention had the greatest impact due to the content provided; the second, third and fourth interventions were ineffectively applied; or that there is a limit that voluntary compliance can achieve. This paper is the first behaviorally-based research that could be found on security awareness. The appearance of the "S" curve and the reasons for it cannot be compared to any previously published results.

The initial baseline for password compliance of forty-four percent is, at first look, a very low number. However, after comparing this number to other studies that have been completed, that percentage is very close to what other studies have found (Stanton, Stam, Mastrangelo and Jolton, 2004; Katz, 2005; and Nyabando, 2006).

When examining all of the interventions employed in this study, the percent of users complying with the password complexity policy rose from an initial baseline of forty-four percent compliant to sixty percent compliant in the final measurement. Decker found that he could not reject his Null Hypothesis and found that there was "no significant correlation" to those end-users who participated in awareness session with those who had not (2006, p. 66). In contrast to Decker's findings, the behaviors measured in this paper show that there is a measureable difference in the level of awareness for those end-users that have participated in security awareness sessions.

As the baseline measurement reflects, forty-four percent of the end-users were voluntarily using compliant passwords. After the administration of four interventions, the percentage of voluntarily compliant passwords rose to sixty percent. One potential reason that Decker could not find a significant correlation is the lack of a behavioral measurement. Decker (2006) used a self-reporting survey to determine end-user compliance with policy as well as attendance in security awareness sessions.

These results show that multiple interventions, while having a statistically significant positive impact on the percent of compliant passwords, failed to achieve a one-hundred percent compliance rate. This failure to reach one-hundred percent compliance through voluntary compliance demonstrates the need to use other hardware or software measures to increase the compliance rate to one-hundred percent. It should be noted that awareness interventions do serve the purpose of providing the knowledge of policy and are still needed. However, to obtain complete compliance with the policy, hardware or software measures appear to be needed.

IMPLICATIONS

Using the results provided by this paper, there are a number of conclusions that can be drawn. The first conclusion is there are varying definitions that have been used for security awareness. These definitions fell short of completely defining security awareness, and as a result, most of the previous research inadequately investigated security awareness. This paper provides a clear, concise definition of security awareness. It is the effort to impart knowledge of or about factors in information security to the degree that it influences users' behavior to conform to policy.

The second conclusion is direct behavioral measurement provides an accurate assessment of an organization's compliance. Previous studies have used self-reporting surveys and questionnaires to assess compliance with policy. This study measures the behavior of end-users by examining the actual end-user passwords, thereby providing accurate and reliable results.

The third conclusion is that voluntary adherence to policy may not provide one-hundred percent compliance. Unless the resulting behavior of the policy is measured directly, the actual compliance rate will be unknown. This study finds that through voluntary compliance, a compliance rate of sixty percent is achieved.

Finally, the fourth conclusion finds that there is a diminishing impact as more interventions are applied to a population. The first intervention performed achieved a fourteen percent rise in compliance. The following three interventions achieved a combined five percent increase. These diminishing impacts demonstrate the need to enforce policies through other means.

The results suggest that it is best to use hardware or software measures to enforce policy. In this particular study, the implementation of the complex password requirement in Active Directory would ensure one-hundred percent compliance.

Recommendations

It is recommended that when possible to use hardware or software to implement and enforce policy. The money that is saved by not repeating ineffective awareness messages can be redirected to those awareness areas that are not enforceable by hardware or software. It is also recommended that behavioral-based measurements used to determine compliance.

Future Research

There are a number of additional questions that warrant research. The first is, are these results generalizable? These interventions and tests should be repeated with a different population. There may be varying levels of effectiveness in different industries. Second, if the interventions were applied in a different order, would the results be the same? If the fourth intervention was administered first, would the same results be achieved? Third, additional research needs to be done on different populations to find the average voluntary compliance

percentage, both before and after the intervention. Finally, behaviorally-oriented studies need to be done on all possible security awareness topics in order to understand the true compliance levels.

AUTHOR INFORMATION

Michael Wolf received the M.S. in Management of Information Systems from the University of Nebraska, Omaha with a concentration in Information Assurance. He received the B.B.A. degree in Management of Information Systems from the University of Iowa. His research interests include information assurance with an emphasis on privacy, education, and cyber defense. He can be reached at mwolfui@gmail.com.

Dwight A. Haworth received his B.S. degree from the United States Air Force Academy, CO, in 1963. He retired from the United States Air Force in 1981. He received his Ph.D. in Management Information from Texas Tech University, Lubbock, TX, in 1990. His research interests are information assurance and systems development and performance. E-mail: haworth@mail.unomaha.edu

Dr. Leah R. Pietron is an Associate Professor in Information Systems and Information Assurance. Her teaching and research focuses in the areas of pedagogy and assessment in Information Systems, Project Management, and Information Assurance. Currently, she is teaching security policy and awareness, risk analysis and management, and project management. E-mail: lpietron@unomaha.edu

REFERENCES

1. Aytes, K. & Connolly, T. (2004). Computer security and risky computing practices: A rational choice perspective. *Journal of Organizational and End User Computing,* Jul-Sep 2004, 22.
2. Conover, W. J. (1980). *Practical Nonparametric Statistics, 2nd Edition*. New York: John Wiley & Sons.
3. Cook, T.D. & Campbell, D. T. (1979). *Quasi-Experimentation: Design & Analysis Issues for Field Settings*. Geneva, Ill.: Houghton Mifflin Company.
4. Decker, L. G. (2008). Factors affecting the security awareness of end-users: A survey analysis within institutions of higher learning (Doctoral dissertation, Cappella University, 2008).
5. Hansche, S. (2001a). Designing a security awareness program: Part I. *Information Systems Security,* January/February 2001, pp. 14-22.
6. Hansche, S. (2001b). Information system security training: making it happen: Part 2. *Information Systems Security*, 10(1), 48-56. Retrieved from Inspec database.
7. Herold, R, (2005). *Managing an Information Security and Privacy Awareness and Training Program*. Boca Raton: Auerbach Publications.
8. Indiana University Information Policy Office (2010). *Campaigns and downloadable media.* Retrieved September 29, 2010 from http://informationpolicy.iu.edu/education/downloads.shtml#ncsam05
9. Information Systems Audit and Control Association (ISACA) (2005). *Security Awareness: Best Practices to Secure Your Enterprise. Rolling Meadows, IL: Information Systems Audit and Control Association.*
10. International Organization for Standardization (ISO) (2005a). ISO/IEC 17799, Information technology - Security techniques - Code of practice for information security management.
11. International Organization for Standardization (ISO) (2005b). ISO/IEC 27001, Information technology - Security techniques - Information security management systems - Requirements.
12. Katz, F. (2005). The effect of a University information security survey on instruction methods in information security. Proceedings of the Information Security Curriculum Conference, USA, 43-49.
13. Krutz, R. L. & Vines, R. D. (2001). *The CISSP Prep Guide, Mastering the Ten Domains of Computer Security*. New York: John Wiley & Sons, Inc.
14. McCumber, J. (2005). *Assessing and Managing Security Risk in IT Systems: A Structured Methodology.* Boca Raton: Auerbach Publications.
15. National Institute for Standards and Technology (NIST) (1996). An Introduction to Computer Security: The NIST Handbook (NIST Special Publication No. 800-12).
16. National Institute for Standards and Technology (NIST) (2003). Building an Information Technology Security Awareness and Training Program (NIST Special Publication No. 800-50).

17. National Institute for Standards and Technology (NIST) (2009). Information Security Training Requirements: A Role- and Performance-Based Model (NIST Special Publication No. 800-16 Revision 1 - Draft).
18. Nyabando, C. J. (2008). An Analysis of Perceived Faculty and Staff Computing Behaviors that Protector Expose Them or Others to Information Security Attacks (Doctoral dissertation, East Tennessee State University, 2008).
19. Okenyi, P., & Owens, T. (2007). On the anatomy of human hacking. *Information Systems Security*, *16*(6), pp. 302- 314.
20. RainbowCrack Project (2010). *RainbowCrack project - crack hashes with rainbow tables.* Retrieved May 1, 2009, from http://project-rainbowcrack.com
21. Rudolph, K. (2009). Implementing a Security Awareness Program. In S. Bosworth, M. E. Kabay & E. Whyne (Eds.), *Computer Security Handbook, 5th edition.* (pp. 49.1-49.42). New York: Wiley.
22. Siponen, M. T. (2000). A conceptual foundation for organizational information security awareness. *Information Management & Computer Security*, 8(1), 31-41.
23. Siponen, M. T. (2001). Five dimensions of information security awareness. *Computers and Society*, June 2001, 24–29.
24. Stanton, J. M., Stam, K. R., Mastrangelo, P. & Jolton, J. (2004). Analysis of end user security behaviors. C*omputers and Security*.
25. Tsohou, A., Kokolakis, S., Karyda, M., & Kiountouzis, E. (2008a). Investigating information security awareness: research and practice gaps. *Information Systems Security*, *17*(5), pp.207-227.
26. Tsohou, A., Kokolakis, S., Karyda, M. & Kiountouzis, E. (2008b). Process-variance models in information security awareness research. *Information Management &Computer Security*, 16(3), pp. 271–287.
27. Willett, K. D. (2008). *Information Assurance Architecture.* Boca Raton: Auerbach Publications.

NOTES

