Association for Information Systems
AIS Electronic Library (AISeL)

SAIS 2012 Proceedings | Southern (SAIS)

2012

Shaming as a Technique for Information Security Policy and Training Adherence

Mark A. Harris
University of South Carolina, marharris1@augusta.edu

SHAMING AS A TECHNIQUE FOR INFORMATION SECURITY POLICY AND TRAINING ADHERENCE

Mark A. Harris
University of South Carolina
maharris@hrsm.sc.edu

ABSTRACT

Information security policy and information security training are vital parts for maximizing information systems security (Dhillon and Backhouse, 2000; Rezgui and Marks, 2008; Siponen, 2001; Straub and Welke, 1998). However, employees not adhering to security policies and not practicing what they learned in training can lead to unintentional mistakes and financial losses for organizations (CSI, 2010). This research investigates Deterrence Theory's shaming as a technique for encouraging employees to adhere more to information security policies and training. Results indicate that employees find peer shaming punishments more severe than typical corporate punishment methods. Implications are that employers using peer shaming as a punishment technique may see better security policy and training adherence.

Keywords

Deterrence theory, shaming, security policy, security training

INTRODUCTION

Information security policy includes the intentions and priorities for protecting an organization's information systems (Karyda, Kiountouzis and Kokolakis, 2005). Security policy is typically created by management and may be influenced by industry standard guidelines, such as ISO/IEC 27002. Information security policy is most commonly taught to employees through information security training (Rotvold, 2008; CSI 2007). Information security training, also known as security awareness training, is a method of educating all employees on how best to protect the firm's information systems (CWS, 2010). Researchers call for information security training to be a primary method for protecting information systems (Rezgui and Marks, 2008; Straub and Welke, 1998). Practitioners seem to be following the advice, as the 2010 Cybersecurity Watch Survey reported that information security training was a top method for protecting information systems (CWS, 2010).

However, a major problem in organizations is getting employees to adhere to information security policy and what they learned in training. Recent research showed that mistakes by employees account for far more financial losses than criminally malicious employees (CSI, 2009, 2010). Over 60% of those surveyed reported financial losses from employees making unintentional blunders, with 14.5% attributing almost all financial losses to employee blunders (CSI, 2010). Twenty-five percent felt that over 60% of their financial losses were due to employee mistakes (CSI, 2009).

So how do managers get employees to adhere to information security policy and what they learned in information security training? Some research has suggested making training more effective by internalizing the material using psychological theories, the format of training, and even video games (Siponen, 2000; Thomson and von Solms, 1998; Cone, Irvine, Thompson and Nguyen, 2007; Shaw, Chen, Harris and Huang, 2009). However, this paper investigates the use of Deterrence Theory and particularly the use of anticipated shaming as a technique for encouraging employee's adherence to information security policy and training. Deterrence Theory research is commonly found in criminology, investigating the reduction of criminal behavior. Creating deterrents, such as fines or even incarceration, is believed to reduce the likelihood of committing crimes.

Deterrence Theory also includes extra-legal sanctions, such as shaming. Criminology research sees shaming as the reaction of respected others to someone that has criminally offended. Anticipated shaming is the internal feelings someone anticipates if respected others find out about the transgression. This paper suggests that anticipated shaming from peers may be a better technique to encourage employees to adhere to information security policy and training than formal corporate sanctions.

The next two sections describe Deterrence Theory and shaming. The research method is then described, followed by the results and discussion. The final section of this paper is the conclusion, which discusses the contribution and limitations of this study.

DETERRENCE THEORY

Deterrence theory has been in practice for thousands of years and in the literature for about 150 years. Proponents of Deterrence Theory believe that "people will engage in criminal or deviant behavior if they do not fear apprehension and punishment" (Keel 2005). Deterrence theory has two major uses: specific deterrence and general deterrence. Specific deterrence is focused on punishing known deviants to keep them from again violating specific norms of society (Keel 2005). A sanction placed against an individual is theorized to reduce the probability of that individual committing the same offense again. General deterrence is focused on reducing deviance in the general population by focusing on future behaviors. People in society are deterred from deviant activities because of their fear of punishment and that fear is reinforced by their knowledge of others getting punished.

The original deterrence theory generally limited punishment to legal sanctions, usually imposed by law enforcement. However, more recent literature (Pogarsky and Piquero, 2004, Nagin and Pogarsky, 2001) has investigated the deterrent effects of extralegal sanctions, such as shame and embarrassment. These types of sanctions often exceed those of formal legal sanction threats (Grasmick and Bursik, 1990).

SHAME AND EMBARRASSMENT

Previous criminology literature suggests that threats of shame and embarrassment function similarly to threats of legal sanctions in preventing criminal behavior (Grasmick, Bursik and Kinsey, 1991). However, the definitions of shame and embarrassment take on different meanings in the literature. Shame was considered a self-imposed sanction of guilt independent of other's reactions to a transgression, where embarrassment was considered a socially imposed sanction stemming from respected others finding out about the transgression (Grasmick, et al., 1991; Grasmick and Bursik, 1990). These definitions are different in that shame does not require one's peers to find out about the criminal behavior and embarrassment does. However, other literature sees shame as a social emotion that requires behavioral reaction from others, such as in the definition of embarrassment (Rebellon et. al., 2010).

Kemper (1990) refers to shame as resulting from one's status decreasing among other actors. Braithwaite (1989, p. 81) stated that "specific deterrence associated with detection from criminal offending works primarily through fear of shame in the eyes of intimates rather than fear of formal punishment." In more recent literature, Rebellon, Piquero, Piquero and Tibbetts (2010) define shaming as the behavioral reactions of others to a criminal who has already offended. This definition of shaming encompasses what previous literature refers to an embarrassment, where the response of peers is involved. Of particular importance to this research, the authors also define "anticipated shaming" as the internal, physiological emotion that a prospective criminal believes might result from a future crime if that crime were to be discovered by intimates. Anticipated shaming is important to this research because it takes into account feelings before a transgression is committed. While shaming research typically investigates criminal behavior, this research will investigate anticipated shaming as a method of encouraging employees to follow information security policies and training. The focus of shaming for this paper will be anticipated shaming from an employee's peer group of coworkers and not management. Management plays a different role with employees and is privy to more information about an employee than other coworkers. For example, managers may have access to an employee's human resource files and other employee records that other coworkers would not be able to access. An employee expects management to have access to such information and that relationship may effect shaming in the eyes of the employee. An employee may not feel the same shame if management were to find out about a transgression versus other coworkers finding out. Therefore, this paper separates shaming from coworkers and shaming from managers and will refer to shaming from coworkers as peer shaming and anything else as non-peer shaming.

RESEARCH METHOD

To investigate how employees feel about peer shaming versus other forms of corporate punishment, an employment background and scenario were created to be used with a survey. Participants were asked to read the background information and scenario before taking the survey. The survey used a 7-point Likert scale to measure one's reaction to various punishments, including several peer shaming punishments and several other possible corporate punishments. Below is the background information and scenario.

Background Information:

You have been working for the same large company for 10 years and you are very happy working there. You get along with everyone and have become friends with many of your coworkers. In fact, you often spend time with your coworkers outside of work. Your coworkers get along well with your other friends and your family.

Scenario:

At work, you just attended an information security awareness training seminar on phishing email. The training explained how to avoid suspicious emails that attempt to trick you into giving out identifying information. A week later, the information technology department management purposely sent all employees a fake phishing email to see if anyone responded to it. You answered the email and gave away your corporate username and password. It was a good thing your information technology department management was testing you because you would have given away important information had the email come from real criminals. It is now being decided how to handle your mistake. Rate the following options for harshness.

The background describes the working environment, where the employee is very happy with their employer and fellow coworkers. It is important to create a positive social environment for the scenario because it establishes a respectful relationship with coworkers that is needed to create shame. In order to have shame, one has to respect the opinion of others that find out about a transgression. Not only does the employee like their coworkers, they socialize outside of work and coworkers get along well with the employee's friends and family. This background information creates a very positive social environment that is perfect for a scenario that measures shaming responses.

The questionnaire that followed the background information and scenario consisted of 12 possible independent reactions management could have to the employee failing to recognize a phishing email. The phishing email resulted in the possibility of sensitive corporate information leaking to outsiders and the mistake is being taken very seriously. Four of the twelve possible management reactions are peer shaming punishments, while the other eight are non-peer shaming punishments. Participants were asked to rate each possible punishment in terms of harshness, where 1 was considered not harsh at all and 7 was considered very harsh. The original list given to participants was given in random order. See table 1 for the ranked list of punishments.

Participants included 71 university students that had experience working for a company with a written set of policies and procedures and some form of security training. Fifty-four were male, seventeen were female and the average age was 22.69 years old.

RESULTS AND DISCUSSION

The average was computed for each of the possible punishments and ranked from one to twelve, with one being the least harsh and twelve the harshest (see Table 1). The least harsh punishment was the employee being told to be more careful by the IT department and the second least harsh punishment was a written warning from a manager. These were not considered peer shaming because the punishment came from management. The third ranked least harsh punishment was that the IT department kept the transgression to themselves and did not tell anyone. It was a little surprising this was not the number one ranked least harsh punishment because it did not even involve a verbal warning.

The harshest punishment was getting fired, which was to be expected given the minimal severity of the transgression. However, the second harshest punishment was posting a photo of those involved on company bulletin boards and in break rooms, which was a surprise. It is interesting because the mean score was 5.61 compared with 5.66 for getting fired. The participants thought having a photo posted was almost as harsh as getting fired and even more harsh than getting demoted (mean score 5.46), the third harshest punishment. The fourth harshest punishment was to have their photo emailed to everyone instead of putting it on bulletin boards. The fifth harshest was being asked to stand up at the next company meeting while everyone is told what you did (mean 4.77). This is somewhat interesting in that everyone gets to see the violator in person and it ranked less harsh than having a photo of the violator emailed or posted. The sixth harshest punishment is emailing a list of violators to all employees (mean 4.44). Standing up at a meeting and being on an email list had means considerably less than the shaming punishments involving photos.

Rank from least harsh to harshest	Mean Score	Possible Punishment	Type of Punishment
1	1.17	The information technology department tells you to be more careful and nobody else finds out.	Non-peer shaming
2	1.39	Your manager gives you a verbal warning in private, but you are not written up.	Non-peer shaming
3	1.45	The information technology department keeps it to themselves and nothing ever happens to you.	Non-peer shaming
4	1.63	You are sent to a more intensive information technology training program.	Non-peer shaming
5	3.23	Your manager writes you up and it goes in your personnel file.	Non-peer shaming
6	4.07	You are required to pay a $50 fine that will be deducted from your next pay check.	Non-peer shaming
7	4.44	A list of those that made the mistake is sent to everyone in the company via e-mail.	Peer Shaming
8	4.77	At the next company meeting, you and others that made the mistake are asked to stand up while management tells everyone what you did.	Peer Shaming
9	5.46	A photo of you and others that made the mistake is sent to everyone in the company via e-mail.	Peer Shaming
10	5.46	You get demoted.	Non-peer shaming
11	5.61	A photo of you and others that made the mistake is posted on company bulletin boards and in break rooms.	Peer Shaming
12	5.66	You get fired.	Non-peer shaming

Table 1. Ranked Punishments

Out of the top six harshest punishments, four are shaming punishments. All of the shaming punishments were considered harsher than paying a $50 fine, getting written up in the personnel file, or having to take more intense training.

What this means is that organizations should consider using shaming as a method for better adherence to information security policies and training. Management needs to be careful not to alienate employees by severely punishing them, such as in the use of photos. If employees consider having their photo posted on a bulletin board (mean 5.61) almost as harsh as getting fired (mean 5.66), the organization might lose employees if it chose that method of punishment. However, management might consider emailing names instead of writing in personnel records or verbal warnings. Because employees consider emailing names (mean 4.44) more harsh than a written entry in the personnel record (mean 3.23) and a verbal warning from management (mean 1.39), there may be better adherence to policies. However, a mean of 4.44 is not considered as harsh as using photos, so perhaps employees will not feel the need to look for employment elsewhere.

Another important idea management needs to consider is the relationship an employee has with coworkers. The shaming technique requires the individual to have a respectful relationship with peers. The scenario's employee got along well with coworkers and they all knew each other outside of work. If an employee does not respect coworkers, shaming might not work because the employee might not care enough about what coworkers. To get the best results from the shaming technique, management should consider building better relationships among employees. Management might consider funding social events for employees or even employee families that bring employees together outside of the daily work environment. If strong relationships can develop among employees, the shaming technique will have a better chance of working.

CONCLUSION

Organizations have a heavy dependence on information security policies and information security training as methods for protecting their information systems. However, mistakes made by employees not following security policy and techniques learned in security training can lead to substantial financial losses for the organization. This paper investigated extralegal sanctions from Deterrence Theory to determine if shaming may help gain better employee adherence to policies and training.

The conclusion is that peer shaming techniques are considered harsher than many other punishments and management should consider using shaming techniques, especially emailing name lists, to get better adherence to information security policies and training. Understanding how employees consider shaming's harshness is the major contribution of this research and may lead to better adherence to an information security policy and training program. Understanding how employees view the severity of various peer shaming techniques in relation to other techniques can help management choose the proper technique for a given situation. Also understanding the employee to coworker relationship and taking steps to strengthen that relationship can increase shaming effectiveness.

The most significant limitation of this research is the sample size and use of university students. Future research should increase the sample size and demographics to include an older workforce. A younger workforce, as in this study, is more apt to use social media and may be more influenced by shaming that uses email and photos than an older workforce. More data will need to be collected to investigate this possibility.

REFERENCES

1. Braithwaite, J. (1989) Crime, shame, and reintegration. Cambridge University Press: Cambridge, UK.
2. Cone, B., Irvine, C., Thompson, M., and Nguyen, D. (2007) A video game for cyber security training and awareness. *Computers and Security*. 26, 63-72.
3. CSI (2007) Computer crime and security survey. Retrieved 3-2-2008 from http://www.gocsi.com/.
4. CSI (2009). Computer crime and security survey. Retrieved 4-30-2010 from http://www.gocsi.com/.
5. CSI (2010) 2010/2011 Computer Crime and Security Survey. Retrieved 4-20-2011 from http://www.gocsi.com/.
6. CWS (2010) Cybersecurity watch survey: cybercrime increasing faster than some company defenses. Retrieved 3-7-2010 from http://www.csoonline.com.
7. Dhillon, G. and Backhouse, J. (2000) Information systems security management in the new millennium, *Communicaitons of the ACM*, 43(7), 125-128.
8. Grasmick, H. G., Bursik, R. J., Jr. (1990) Conscience, significant others, and rational choice: Extending the deterrence model, *Law Society Review*, 24, 837-861.
9. Grasmick, H. G., Bursik, R., Kinsey, K. (1991) Shame and embarrassment as deterrents to noncompliance with the law, *Environment and Behavior*, 23(2), 233-251.
10. Karyda, M., Kiountouzis, E., and Kokolakis, S. (2005) Information systems security policies: A contextual perspective, *Computers and Security*, 24, 246-260.
11. Keel, R. (2005) Rational choice and deterrence theory. Retrieved 3-7-2010 from: http://www.umsl.edu/~rkeel/200/ratchoc.html, p. 1-4.
12. Kemper, T. D. (1990) Social relationship and emotions: A structural approach. In T. D.
13. Kemper (Ed.) Research agendas in the sociology of emotions (pp. 207−237). New York: SUNY Press.
14. Nagin, D. and G. Pogarsky. (2001) Integrating celerity, impulsivity, and extralegal sanction threats into a model of general deterrence: Theory and evidence, *Criminology*, 39 (4): 865-888.
15. Pogarsky, G., A. R. Piquero, et al. (2004) Modeling change in perceptions about sanction threats: The neglected linkage in deterrence theory, *Journal of Quantitative Criminology*, 20(4), 343-369.
16. Rebellon, C., Piquero, N., Piquero, A., Tibbetts, S. (2010) Anticipated shaming and criminal offending, *Journal of Criminal Justice*, 38, 988-997.
17. Rezgui, Y. and Marks, A. (2008) Information security awareness in higher education: An exploratory study, *Computers and Security*, 27, 241-253.
18. Rotvold, G. (2008) How to create a security culture in your organization, *Information Management Journal*, 42(6), 32.
19. Shaw, R., Chen, C., Harris, A., and Huang, H. (2009) The impact of information richness on information security awareness training effectiveness, *Computers and Education*. 52, 92-100.
20. Siponen, M. (2000). A conceptual foundation for organizational information security awareness, *Information Management and Computer Security*, 8(1), 31-41.
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, Dhillon, G. (ed.) (pp. 101–124), Hershey, PA: Idea Group Publishing.

22. Straub, D. and Welke, R. (1998) Coping with systems risks: Security planning models for management decision making, *MIS Quarterly*, 22, 441–469.
23. Thomson, M. and Von Solms, R. (1998). Information security awareness: educating your users effectively, *Information Management and Computer Security*, 6(4), 167.