Proceedings of the 53rd Hawaii International Conference on System Sciences | 2020

Understanding the Role of Incentives in Security Behavior

Sanjay Goel
UAlbany, SUNY
goel@albany.edu

Kevin Williams
UAlbany, SUNY
kwilliams@albany.edu

Jenny Huang
UAlbany, SUNY
Jhuang2@albany.edu

Merrill Warkentin
Mississippi State U.
m.warkentin@msstate.edu

Abstract

A key challenge for researchers has been to affect change in user security behavior in organizations. Several theories from different domains have been used for understanding and changing user security behavior including deterrence, fear appeals, and education; however, the success of these approaches has been low. In this research we examine the role of financial incentives in changing user behavior; we specifically provide incentives to users for good security practices. The study attempts to switch user behavior such that they adopt good security habits however it recognizes the limitations of extrinsic rewards in being temporary and couples the extrinsic rewards to affect intrinsic motivation through use of nudges. The field study shows positive results however the number of subjects in our study was small (24). Our goal is to extend the study by large scale data collection to further validate our results.

1. Introduction

The threat and impact of cybersecurity breaches are observed throughout society, from 2.5 million security clearance files compromised at a government agency to huge consumer data losses at EBay, Anthem, Sony, Target, JP Morgan, and other companies. Employees are widely recognized as the weakest link in an organization's cybersecurity practice. Yet current programs designed to improve employee security behaviors often fail because interventions are not viewed as personally relevant (Johnston et al., 2019a, 2019b). Our study addresses a significant gap in scientific investigations of user cybersecurity hygiene by providing direct financial incentives to motivate users to comply with organizational cybersecurity policies and procedures. In addition, we tested the effect of psychological manipulations (nudges) in sustaining compliance.

Research points to the organizational insider, typically the employee or contractor, as a key threat to the security of information, and inspires the perennial organizational mandate of decreasing that risk (Im and Baskerville 2005; Stanton et al. 2005; Guo et al. 2011, Warkentin and Willison 2009; Willison and Warkentin 2013). Insider threats can manifest from carelessness, apathy, or malicious behavior. The recent dramatic rise in personal mobile devices in the workplace and third-party applications has introduced even more potential vectors for data leakage from employee carelessness and noncompliance. Private and public-sector enterprises are coming to grips with the increased risks of the bring your own device (BYOD) phenomenon, with employees exhibiting a lack of caution as devices, formats, and connectivity proliferate, and data crosses previously demarcated personal, public, and professional lines. In its survey of more than 500 employees at mid-to-large companies, Centrify found that forty-three percent have accessed sensitive corporate data while on an unsecured public network (Kaneshige, 2014).

No significant improvement in these trends has been realized, despite a range of approaches designed and implemented to improve employee security compliance. Methods range from implementing information security policies, to security education training and awareness (SETA) campaigns, to online monitoring and fear-based approaches, to punitive measures. Mutchler and Warkentin (2015) note that awareness programs are frequently deemed as an ineffective and unproductive use of corporate funds. A 2014 Information Security Forum survey noted that 75% of its member organizations have an ongoing security awareness program, but only 15% report having reached the level of awareness and improvement that they were striving for. The limitations of standard security awareness warnings and programs have been well documented (see Dhamija et al., 2006; Sunshine et al.. 2009; Whitten and Tyger, 1998, etc.). We argue that the limited effectiveness of security interventions is partially due to a failure to properly incentivize user behavior.

The dominant theoretical frameworks used by researchers to improve information security have been

URI: https://hdl.handle.net/10125/64261
978-0-9981331-3-3

Protection Motivation Theory (Rogers, 1975; 1983) and Deterrence Theory (Straub, 1990; Straub and Welke, 1998). These theories suggest that users make rational security decisions by cognitively weighing the relative gains and losses associated with their choices within a decision calculus. They assume that users will respond rationally to perceived security threats in the environment and to sanctions imposed on noncompliance. Users are expected to internally regulate their behavior based on an understanding of security threats and the consequences of risky behavior. However, in the course of daily work activities, users may minimize the risks associated with their behavior, may rationalize noncompliant behavior, and may feel that the costs of compliance outweigh perceived benefits. Neither intrinsic nor extrinsic incentives discussed in the literature to motivate compliance with security policies have been very effective. A recent meta-analysis (Cram et al., 2019) found that rewards only have a small effect on policy compliance. The authors included both tangible (e.g. prizes) and intangible (e.g. acknowledgement of the supervisor) rewards in this category. It is still unclear how monetary rewards will impact users' compliance with policies. We expect monetary rewards to have a stronger effect than other types of rewards, because it "prices" the compliance behaviors and gives users a clear value. We propose altering user behavior and increasing compliance by changing the security decision calculus. Drawing on principles of behavioral economics, we used extrinsic rewards (i.e. financial incentives) to initiate compliance, and psychological manipulations (nudges) to promote ongoing internal regulation of security behavior, such that users sustain secure behaviors when incentives are no longer in place.

2. Literature

Where Protection Motivation Theory and Deterrence Theory emphasize rational decision making as the basis for behavior change, the field of behavioral economics focuses on the cognitive, social, and emotional factors that influence the choices that people make in particular contexts.

The lack of efficacy in security programs lies squarely in the gap between user motivation and compliance, or intention and execution. Acquisti and Grosslags (2004) showed that while most users profess a strong desire to have and maintain secure systems, they also show a surprising willingness to divulge personal information for as little as $0.25. Christin (2011) provided minimal financial incentives to users willing to download unknown executables. Results demonstrated that, in direct opposition to their stated preferences, most users do not attach an economic value to the security of their systems: 70% of all participants in the study understood that running unknown programs could be dangerous, yet all chose to do so once paid. In addition, users often feel that the effort needed to comply with security policy outweighs the rewards associated with compliance. Beautement et al. (2009) coined the term the 'compliance budget' to refer to the reasonable amount of effort that employees are willing to expend to keep the organization safe. Muraven et al. (2008) note that the tasks related to compliance require users to tap a limited amount of "vitality" that is needed for self-control, thereby depleting the reserves for future activities. In general, functionality often overshadows security in terms of prioritizing the tasks at hand.

Financial incentives have long been assumed to affect behavior and performance. Behaviorists and economists argue that financial incentives exert a strong influence on worker effort, persistence, and performance. These assumptions have been supported by research. In a review of organizational research, Ilgen (1990) found positive relationship between financial incentives offered to workers and performance. Pay-for-performance systems have generally been successful in improving the quantity of performance, if not the quality (Baker et al., 1988; Jenkins et al., 1998). Camerer and Hogarth (1999) found that the positive effects of financial incentives are strongest for tasks in which effort and performance are closely linked.

Despite generally positive results, the use of extrinsic incentives has been criticized by researchers for several reasons. Behavior that occurs in the presence of a reward is unlikely to be sustained when it is withdrawn. This suggests that once financial incentives are instituted, they must be maintained to ensure desired results. Prolonged use of financial incentives can be costly to organizations, so changes in behavior need to be strong enough to ensure a positive return on investment. Psychologists and behavioral economists have also identified unintended consequences of financial rewards; rewards may increase target behaviors while reducing other desirable behaviors (e.g., quality) or may inadvertently increase undesirable behaviors (e.g., cheating) (Kerr, 1975). Other psychologists argue that financial incentives undermine intrinsic motivation, which is seen as essential for prolonged effort and interest in an activity. Intrinsic motivation refers to actions that are inherently interesting or enjoyable, whereas extrinsic motivation refers to actions that lead to outcomes that are separate from the activity itself (e.g., money, praise; Ryan & Deci, 2000). Intrinsic motivation is a

powerful source of motivation that sustains engagement and effort over extended periods of time without the need for "external prods, pressures, or rewards" (Ryan & Deci, 2000, p. 56). However, it is most relevant for explaining behaviors that are exploratory, curiosity-driven, or associated with play. Workers can hardly be seen as intrinsically motivated to follow security policies; security-related tasks are not designed to be intrinsically interesting and thus require some type of extrinsic motivation. The challenge is to prevent or mitigate the negative and unintended consequences of extrinsic motivation noted above.

The goal of this research is to provide an incentive that is powerful enough to motivate users to comply with security policies, and then identify psychological nudges that can sustain compliance. We used financial incentives to "flip the switch," to increase user motivation to act safely. We first used financial incentives because the existing literature suggests that intrinsic and social incentives are not operating strongly in the typical security context. Analogous to investing in wellness programs to manage corporate healthcare costs; incentive programs could prove an economical way to reduce breaches and overall security costs. Beyond encouraging secure behaviors, incentives directly and positively acknowledge the importance of the user's personal decisions to the security of the overall network. However, relying on financial incentives may not be a viable long-term solution to an organization's security problems. It is also important to find ways to promote ongoing internal regulation of security behavior and we do this through use of nudges to sustain the behavior.

3. Research Design

The participants were employees from a local company that develops software for the management of enterprise information. There were 27 employees who volunteered to participate in the study. Among these participants, one was aware about our study purpose and hypotheses, one left the company in the middle of the study, and one never responded to our emails. Thus, the data from these three employees were removed from data analysis, resulting in 24 valid cases (17 males and 7 females, mean age = 33.22, S.D. = 9.51) used for analyses. There was a variety in participants' positions, including software engineer, QA analyst, bookkeeper, client manager, etc.

We obtained informed consent from participants before data collection was started. The procedure of the study was introduced to the participants, and they were informed that all evaluations on their information security behaviors would be in accordance with their company's policies, and they had the right to quit the study any time without penalties. In addition, in order to track participants' responses to phishing emails, we sent faking phishing emails to the participants. But the participants were not informed that they would receive phishing emails from us. Two phishing emails were sent to the participants' work email address per week at random days and time. The phishing emails vary in the level of work-contextualization and individualization. Two trained graduate students rated the emails on the level of contextualization. More work-contextualized emails contain more cues that indicate a specific workplace setting or are more related to the receiver's work role. The interrater agreement is good between the two raters (ICC [A,2] = .839). We thus used the averaged rating as an indicator of the level of contextualization. An example of a none or slightly contextualized phishing email is an email sent by a bank notifying an abnormal account activity. An example of a highly contextualized phishing email is an email notifying receiver of an active threat to company server. One contextualized and one non-contextualized phishing email were sent to participants each week. In addition, one of the four emails that participants receive every two weeks was individualized. Individualization was manipulated by including the email receiver's name in the content. All data were encrypted and delivered to the research team directly and no person in the company had access to the data of participants.

The first two week's behavioral data were used as a baseline. In the third week, a 30-minute training session was provided to the participants by the company's IT person to help them review the company's policies, which includes protection of hardcopy documents, safe internet usage, safe email behaviors, software installation and updates, account safety, and use of removable storage. The participants were provided with a hardcopy of the notes and a list of behaviors that would be tracked and evaluated in the study. The reward program started from the fifth week. The participants could gain at maximum 50 dollars per week if they fully complied with the company's policies, 40 dollars if one violation was detected, 30 dollars if two violations, 20 dollars if three violations, and zero dollars if more than three violations. Feedback on participants' behaviors from the previous week and the accumulated amount of monetary reward was provided starting from week 6. The reward program lasted for 12 weeks and ended at the end of the 17th week of the study. Each participant received a check issued by the researchers' institution.

Both rewards and feedback were removed starting from week 18. We kept collecting data on participants' information security behaviors to examine if their behaviors retained after the removal of rewards. In weeks 20 and 21, we sent nudges through emails to the participants on Monday, Wednesday, and Friday mornings to remind them to follow the company's information security policies. The nudges read as "*** employees are continuing to practice careful and safe cybersecurity behaviors. Keep up the good work!" Then in week 22, we removed nudges again.

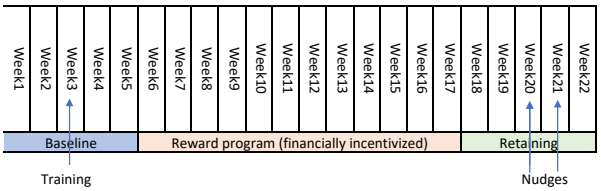

Figure 1: Experimental Timeline

Data were collected on several metrics: 1) strength of passwords, measured with a brute-forced password cracking tool; 2) time and number of clicks on phishing emails, and whether the links embedded in the emails were clicked; and 3) number of times non-work emails were used on work computer, which was measured with users' webpage visiting log.

4. Results

All participants' passwords were tested through a brute-forced cracking tool and were considered weak if cracked. Each week we calculated the number of employees that had a password that was easily cracked. Figure 2 shows the trend in employees' behaviors. In the first two weeks of the study, there were four participants who used weak passwords. After the training that was provided in week 3, there was a drop-off in the number of participants who set weak passwords. That number lowered to 1 at week 5, when the reward program started. Because the company's computer system forces the employees to reset passwords every three months, there were a couple new weak passwords detected during the period of reward program (week 6-17). However, starting from week 14, the number of participants who had weak passwords dropped down to zero and remained at zero thereafter. Our results showed that monetary incentive did have an effect on improving people's password security behaviors, although there is some time lag between the initiate of incentive and when full compliance was reached.

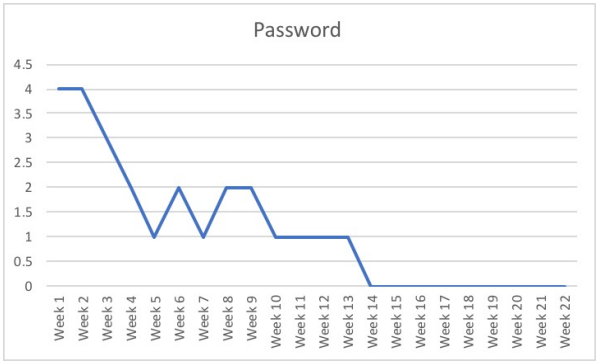

Figure 2. Number of participants who set weak passwords.

The number of times the phishing emails were opened remained at a relatively low level during the whole period of study. To start from, the baseline of clicks was low, with no participants opening the phishing emails we sent in the first five weeks (No phishing emails were sent during the training week – week 3). The first peak appeared in week 8. There were two participants who opened the phishing email titled "Sorry about sending this late" (average contextualization rating = 4.5 on a 1-5 scale, individualized). The second peak was in week 16, with one participant opening the phishing email titled "Job opportunity" (average contextualization rating = 3.5 on a 1-5 scale, non-individualized). After the rewards were removed, there seemed to be an increase in the number of participants who opened the phishing emails. In week 20, when rewards were removed while nudges were in place, there was one participant who opened the email titled "Reminder: Online meeting starts in 1 day" (average contextualization rating =4 on a 1-5 scale, non-individualized), and another 4 participants who opened the emails titled "Verify your email address" sent from a fake Apple customer service account (average contextualization rating = 1 on 1-5 scale, individualized). However, none of the participants who opened the phishing emails went one step further to click the links embedded in the emails. Partly due to the nature of the company business which both contractually and legally obliges its employees to protect the data they possess, it seems employees in this local company already had high levels of awareness of and good practice regarding phishing emails. However, we did notice an increase in the number of people who opened phishing emails after the incentives were removed (week 20). In addition, most of the phishing emails that were opened by participants were designed to be work-relevant.

Figure 3. Number of participants who opened phishing emails.

Figure 4 shows the number of people who used non-work emails. In the first 5 weeks, before incentive program came into effect, the number of participants who opened non-work emails were relatively high. There was a significant drop in week 6, when the reward program started. However, the number went back to a level comparable to that before reward program started since week 7. The significant drop appeared in week 10 and the number of people who used non-work emails remained relatively low thereafter. This trajectory of behavioral change is similar to that of password practice. Incentives did show an effect on influencing people's behavior but took some time to reach its maximum effect.

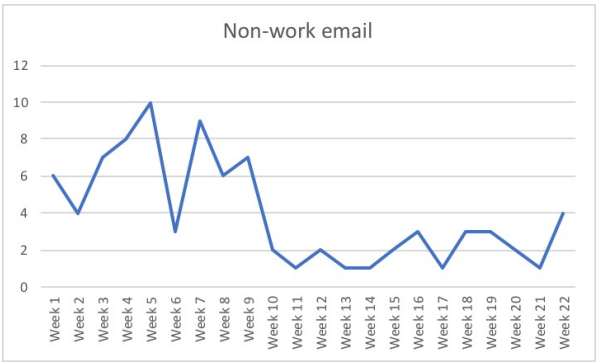

Figure 4. Number of participants who used non-work emails on work computers.

5. Conclusions

The research goal was to investigate whether incentives can be used to promote behavior change leading to improved compliance with security guidelines and processes. Our sample was a small forensics firm with about 70 employees; however, our valid sample size was small with 24 individuals. The results indicate a clear shift in safe password practice and the use of non-work email due to incentives compared to the baseline security behavior. Follow-up study post incentives, during which nudges were given, showed some signs of increase in employees' non-compliance but the compliance level was generally higher than that before the incentive program started. However, the results need to be interpreted with caution because the follow-up stage was relatively short and that we only tested nudges for two weeks, which prevents us from making a strong conclusion. A larger study is now planned to understand the role of incentives further as well as to clarify the role of nudges in sustaining the behavior.

10. References

[1] Acquisti, A., & Grossklags, J. (2004). Privacy attitudes and privacy behavior. In *Economics of information security* (pp. 165-178). Springer US.

[2] Baker, G.P., Jensen, M.C., & Murphy, K.J. (1988). Compensation and incentives: Practice vs. theory. *Journal of Finance*, 43, 593-616.

[3] Beautement, A., Sasse, M. A., & Wonham, M. (2009, August). The compliance budget: managing security behaviour in organisations. In *Proceedings of the 2008 Workshop on New Security Paradigms* (pp. 47-58). ACM.

[4] Camerer, C.F. & Hogarth, R.M. (1999). The effects of financial incentives in experiments: A review and capital-labor-production framework. *Journal of Risk and Uncertainty*, 19, 7-42.

[5] Christin, N. (2011). Network Security Games: Combining Game Theory, Behavioral Economics, and Network Measurements. *Decision and Game Theory for* Security: Lecture Notes in Computer Science, 7037, 4-6.

[6] Cram, W. A., D'Arcy, J., & Proudfoot, J. G. (2019). Seeing the Forest and the Trees: A Meta-Analysis of the Antecedents to Information Security Policy Compliance. *MIS Quarterly*, 43(2), 525-554.

[7] Dhamija, R., Tygar, J. D., & Hearst, M. (2006, April). Why phishing works. In *Proceedings of the SIGCHI conference on Human Factors in computing systems* (pp. 581-590). ACM.

[8] Guo KH, Yuan YN, Archer P, Connelly CE (2011) Understanding nonmalicious security violations in the workplace: A composite behavior model. *Journal of Management Information Systems 28(2)*, 203-236.

[9] Ilgen, D. (1990). *Pay for performance: Motivational issues*. Working paper prepared for the Committee on Performance Appraisal for Merit Pay. Washington, DC: National Research Council.

[10] Im, G. P., & Baskerville, R. L. (2005). A longitudinal study of information system threat categories: the enduring problem of human error. *ACM SIGMIS DATABASE of Advances in Information Systems*, *36*(4), 68-79.

[11] Jenkins, G.D., Mitra, A., Gupta, N., & Shaw, J. (1998). Are financial incentives related to performance? A

meta-analytic review of empirical research. *Journal of Applied Psychology*, 83(5), 777-787,

[12] Johnston, A.C., M. Warkentin, A.R. Dennis, and M. Siponen. (2019a). Speak their language: Designing effective messages to improve employees' information security decision making. *Decision Sciences*, forthcoming (published online 23 July 2018 at https://onlinelibrary.wiley.com/doi/abs/10.1111/deci.12328).

[13] Johnston, A.C., M. Warkentin, and M. Siponen. (2019b) . An Enhanced Fear Appeal Framework: Leveraging Threats to the Human Asset through Sanctioning Rhetoric. *MIS Quarterly*, 39(1), 113-134.

[14] Kaneshige, T. (2014). What is going wrong with BYOD. *CIO. com*. Retrieved from http://www.cio.com/article/2375498/byod/what-is-going-wrong-with-byod-.html

[15] Kerr, S. (1975). On the folly of rewarding A, while hoping for B. *Academy of Management Journal*, 18(4), 769-783.

[16] Muraven, M., Gagné, M., & Rosman, H. (2008). Helpful self-control: Autonomy support, vitality, and depletion. *Journal of Experimental Social Psychology*, *44*(3), 573-585.

[17] Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change1. *The Journal of Psychology*, *91*(1), 93-114.

[18] Rogers, R. W. (1983). Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation. In J. T. Cacioppo & R. E. Petty (Eds.), *Social psychophysiology: A sourcebook.* London: Guilford Press.

[19] Ryan, R.M. & Deci, E.L. (2000). Intrinsic and extrinsic motivations: Classic definitions and new directions. *Contemporary Educational Psychology*, 25, 54-67.

[20] Stanton, J. M., Stam, K. R., Mastrangelo, P., & Jolton, J. (2005). Analysis of end user security behaviors. *Computers & Security*, *24*(2), 124-133.

[21] Straub Jr, D. W. (1990). Effective IS security: An empirical study. *Information Systems Research*, *1*(3), 255-276.

[22] Straub, D. W., & Welke, R. J. (1998). Coping with systems risk: security planning models for management decision making. *MIS Quarterly*, 441-469.

[23] Sunshine, J., Egelman, S., Almuhimedi, H., Atri, N., & Cranor, L. F. (2009, August). Crying Wolf: An Empirical Study of SSL Warning Effectiveness. In *USENIX Security Symposium* (pp. 399-416).

[24] Warkentin, M., & Willison, R. (2009). Behavioral and policy issues in information systems security: the insider threat. *European Journal of Information Systems*, *18*(2), 101-105.

[25] Willison, R., and Warkentin, M. (2013). "Beyond Deterrence: An Expanded View of Employee Computer Abuse," *MIS Quarterly* (37:1), 1-20.

[26] Whitten, A., & Tygar, J. D. (1998). *Usability of security: A case study* (No. CMU-CS-98-155.